

# Deciding Irreducibility/Indecomposability of Feedback Shift Registers is **NP**-hard

Lin WANG

*Science and Technology on Communication Security Laboratory*

*Chengdu 610041, P. R. China*

*Email: linwang@math.pku.edu.cn*

## Abstract

Feedback shift registers(FSRs) are a fundamental component in electronics and secure communication. An FSR  $f$  is said to be reducible if all the output sequences of another FSR  $g$  can also be generated by  $f$  and the FSR  $g$  has less memory than  $f$ . An FSR is said to be decomposable if it has the same set of output sequences as a cascade connection of two FSRs. It is proved that deciding whether FSRs are irreducible/indecomposable is **NP**-hard.

*Key words:* feedback shift registers, irreducible, indecomposable, **NP**-hard, Boolean circuit, cycle structure

## 1 Introduction

Feedback shift registers are broadly used in spread spectrum radio, control engineering and confidential digital communication. Consequently, this subject has attracted substantial research over half a century. Particularly, feedback shift registers play a significant role in the stream cipher finalists of the eSTREAM project [10].

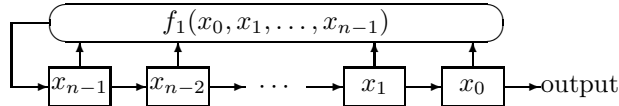


Figure 1: A feedback shift register with feedback logic  $f_1$

As shown in Figure 1, an  $n$ -stage *feedback shift register*(FSR) consists of  $n$  bit registers  $x_0, x_1, \dots, x_{n-1}$  and an  $n$ -input feedback logic  $f_1$ . The vector  $(x_0(t), x_1(t), \dots, x_{n-1}(t))$  is called a *state* of this FSR, where  $x_i(t)$  is the value of  $x_i$  at clock cycle  $t$ ,  $0 \leq i < n$ . The state at clock cycle 0 is called the *initial state*. Along with clock impulses the values stored in bit registers update themselves as

$$(x_0(t+1), x_1(t+1), \dots, x_{n-1}(t+1)) = (x_1(t), \dots, x_{n-1}(t), f_1(x_0(t), x_1(t), \dots, x_{n-1}(t))), \quad (1)$$

and the map defined by Eq.(1) is called the *state transformation* of this FSR.

The  $(n+1)$ -input Boolean function  $f(x_0, x_1, \dots, x_n) = x_n \oplus f_1(x_0, x_1, \dots, x_{n-1})$ , where  $\oplus$  denotes exclusive-or, is called the characteristic function of the FSR in Figure 1, and without ambiguity we also denote this FSR by  $f$ . Let  $G(f)$  denote the set of sequences generated by  $f$ , i.e.,

$$G(f) = \{s \in \{0, 1\}^* : \forall t, f(s(t), s(t+1), \dots, s(t+n)) = 0\},$$

where  $\{0, 1\}^*$  is the set of binary sequences. If  $f(x_0, x_1, \dots, x_n) = x_n \oplus c_{n-1}x_{n-1} \oplus \dots \oplus c_1x_1 \oplus c_0x_0$ , where  $c_0, c_1, \dots, c_{n-1} \in \{0, 1\}$ , then  $f$  is called a *linear feedback shift register (LFSR)*, and  $p(x) = x^n \oplus c_{n-1}x^{n-1} \oplus \dots \oplus c_1x \oplus c_0$  is called its *characteristic polynomial*. Without ambiguity we also denote this LFSR by  $p(x)$ . An FSR which is not an LFSR is called a *nonlinear feedback shift register (NFSR)*.

If there exists an  $m$ -stage FSR  $g$  such that  $m < n$  and  $G(g) \subset G(f)$ , then  $g$  is called a *subFSR* of  $f$  and  $f$  is said to be *reducible*. Otherwise,  $f$  is said to be *irreducible*.

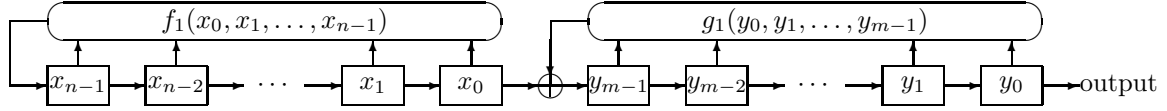


Figure 2: The cascade connection of  $f$  in  $g$

Let  $f(x_0, x_1, \dots, x_n) = x_n \oplus f_1(x_0, x_1, \dots, x_{n-1})$  and  $g(y_0, y_1, \dots, y_m) = y_m \oplus g_1(y_0, y_1, \dots, y_{m-1})$  be two FSRs. The finite state machine in Figure 2 is called the *cascade connection* of  $f$  into  $g$ . The Grain family ciphers use the cascade connection of an LFSR into an NFSR [5]. Green and Dimond [4] defined the *product FSR*<sup>1</sup> of  $f$  and  $g$  to be

$$(f * g)(x_0, x_1, \dots, x_{n+m}) = f(g(x_0, x_1, \dots, x_m), g(x_1, x_2, \dots, x_{m+1}), \dots, g(x_n, x_{n+1}, \dots, x_{n+m})),$$

and showed  $G(f; g) = G(f * g)$ , where  $G(f; g)$  is the set of output sequences of the cascade connection of  $f$  into  $g$ . Given an FSR  $h$ , if there exist two FSRs  $f$  and  $g$  satisfying  $h = f * g$ , then  $h$  is said to be *decomposable*. Otherwise,  $h$  is said to be *indecomposable*.

It is appealing to decide whether an FSR is (ir)reducible/(in)decomposable for the reasons below. First, it offers a new perspective on analysis of stream ciphers. Notice that all sequences generated by  $g$  is also generated by  $f * g$  if  $f$  can output the 0-sequence. A reducible/decomposable FSR in unaware use may undermine the claimed security of stream ciphers, e.g., causing inadequate period of the output sequences. Particularly, if  $g$  is an LFSR and  $f$  can output the 0-sequence, then  $f * g$  can generate a family of linear recurring sequences, vulnerable to the Berlekamp-Massey algorithm. Second, it potentially improves implementation of FSRs. On one hand, it costs less memory to replace an FSR with its large-stage subFSR, if there is one, while generating a great part of its output sequences. On the other hand, similar to the idea of Dubrova [2], substituting a decomposable FSR by its equivalent cascade connection as in Figure 2 possibly reduces the circuit depth of the feedback logics, in favor of less propagation time and larger throughput. Third, an algorithm testing (ir)reducibility/(in)decomposability helps to design useful FSRs. Because Tian and Qi [12] proved that on average at least one among three randomly chosen NFSRs is irreducible, a great number of irreducible NFSRs can be found if deciding irreducibility of FSRs is feasible. Besides, FSRs generating maximal-length sequences were constructed based on inherent structure of decomposable FSRs [9].

Two algorithms were proposed by [11] to find affine subFSRs of NFSRs. By [6], if an NFSR  $h$  is decomposed as the cascade connection of an LFSR  $f$  into an NFSR  $g$  and  $f$  is primitive with stage no less than that of  $g$ , then all affine subFSRs of  $h$  are actually those of  $g$ . (In)decomposability of LFSRs is completely determined by their characteristic polynomials. By [4, 7, 13], an LFSR  $h$ , with its characteristic polynomial  $p(x)$ , is decomposed as  $h = f * g$  if and only if  $f$  and  $g$  are LFSRs and  $p(x) = l_1(x) \cdot l_2(x)$ , where  $l_1(x)$  and  $l_2(x)$  are characteristic polynomials of  $f$  and  $g$ , respectively. In contrast, decomposing NFSRs seems much more challenging, though some progress has been made recently. Using the language of algebraic normal forms of Boolean functions, Ma *et al* [8] gave an algorithm to decompose NFSRs into the cascade connection of an NFSR into an LFSR, and Tian and Qi [13] gave a series of algorithms to decompose NFSRs into the cascade connection of two NFSRs. Noteworthily, Zhang *et al* [14] gained an algorithm decomposing an NFSR  $f$  into the cascade connection of an NFSR into an LFSR, and the complexity of their algorithm is polynomial in

<sup>1</sup> The product FSR of  $f$  and  $g$  is denoted by  $f.g$  in [4], while by  $f * g$  in [9]. We follow the latter in order to avoid ambiguity with periods or conventional multiplication.

the size of the algebraic normal form of  $f$  and the size of the binary decision diagram of  $f$  if converting the algebraic normal form of  $f$  to the binary decision diagram of  $f$  is polynomial-time computable.

*Our contribution.* This correspondence studies irreducibility and indecomposability from the perspective of computational complexity. **NP** is the class of all problems computed by polynomial-time nondeterministic Turing machines. A problem is **NP-hard** if it is at least as hard as all **NP** problems. This correspondence proves that deciding whether an FSR is irreducible(indecomposable) is **NP-hard**.

The rest of this paper is organized as follows: In Section 2 we prepare some notations, basic facts on Boolean circuits and some lemmas on the cycle structure of FSRs. **NP-hardness** of FSR irreducibility and FSR indecomposability is shown in Sections 3 and 4, respectively. The last section includes a summary and a comment on future work.

## 2 Preliminaries

### 2.1 Notations

Throughout this paper,  $\mathbb{Z}$  denotes the set of integers, “+” addition of integers, and “ $\oplus$ ” the exclusive-or(XOR) operation.

Denote  $\mathbf{1}^m = (1, 1, \dots, 1) \in \{0, 1\}^m$ ,  $\mathbf{0}^m = (0, 0, \dots, 0) \in \{0, 1\}^m$  and  $\boldsymbol{\iota}^m = (1, 0, \dots, 0) \in \{0, 1\}^m$ . For  $\mathbf{u} \in \{0, 1\}^m$ , denote  $\bar{\mathbf{u}} = \mathbf{u} \oplus \mathbf{1}^m$  and  $\hat{\mathbf{u}} = \mathbf{u} \oplus \boldsymbol{\iota}^m$ .

For  $\mathbf{u} = (a_1, a_2, \dots, a_m) \in \{0, 1\}^m$  and  $1 \leq k < m$ , let

$$\begin{aligned} [\mathbf{u}]_k &= (a_1, a_2, \dots, a_k) \in \{0, 1\}^k; \\ [\mathbf{u}]_k &= (a_{m-k+1}, a_{m-k+2}, \dots, a_{m-1}, a_m) \in \{0, 1\}^k. \end{aligned}$$

For  $\mathbf{u} = (a_1, \dots, a_k) \in \{0, 1\}^k$  and  $\mathbf{v} = (b_1, \dots, b_m) \in \{0, 1\}^m$ , denote  $\mathbf{u} \parallel \mathbf{v} = (a_1, \dots, a_k, b_1, \dots, b_m) \in \{0, 1\}^{k+m}$ .

Without ambiguity a vector  $(a_0, a_1, \dots, a_{m-1}) \in \{0, 1\}^m$  is uniquely taken as the nonnegative integer  $\sum_{j=0}^{m-1} 2^j a_j$ . Thereby, the natural order relation on  $\{0, 1\}^m$  is imposed, i.e.,  $(a_0, a_1, \dots, a_{m-1}) < (b_0, b_1, \dots, b_{m-1})$  if and only if  $\sum_{j=0}^{m-1} 2^j a_j < \sum_{j=0}^{m-1} 2^j b_j$ .

### 2.2 Boolean circuits

An  $m$ -input *Boolean circuit*  $f$  is a directed acyclic graph with  $m$  sources and one sink [1]. The value(s) of source(s) is(are) input(s) of the Boolean circuit; Any nonsource vertex, called a *gate*, is one of the logical operations OR( $\vee$ ), AND( $\wedge$ ) and NOT( $\neg$ ), where the fan-in<sup>2</sup> of OR and AND is 2 and that of NOT is 1; The value outputted from a gate is obtained by applying its logical operation on the value(s) inputted into it; The value outputted from the sink is the output of the Boolean circuit  $f$ . The size of the circuit  $f$ , denoted by **SIZE**( $f$ ), is the number of vertices in it. An  $m$ -input Boolean circuit  $f$  is *satisfiable* if there exists  $\mathbf{v} \in \{0, 1\}^m$  such that  $f(\mathbf{v}) = 1$ .

**PROBLEM:** CIRCUIT SATISFIABILITY

INSTANCE: A Boolean circuit  $f$  with its size **SIZE**( $f$ ).

QUESTION: Is  $f$  satisfiable?

A decision problem in **NP** class is **NP-complete** if it is not less difficult than any other **NP** problem.

**Lemma 1.** [1] *The CIRCUIT SATISFIABILITY problem is NP-complete.*

---

<sup>2</sup>The fan-in of a gate is the number of bits fed into it.

A decision problem  $P$  is *polynomial-time Karp reducible* to a decision problem  $Q$  if there is a polynomial-time computable transformation  $T$  mapping instances of  $P$  to those of  $Q$  such that an instance  $x$  of  $P$  answers yes if and only if  $T(x)$  answers yes [1]. A decision problem is **NP-hard** if a **NP**-complete problem is polynomial-time Karp reducible to it [1].

An FSR is completely characterized by its feedback logic. We use Boolean circuits to characterize the feedback logic of FSRs for the following two reasons<sup>3</sup>. First, FSRs are mostly implemented with silicon chips, and the Boolean circuit is an abstract model of their feedback logic in silicon chips. Second, the Boolean circuit is a generalization of Boolean formula [1]. Therefore, in this correspondence the size of an FSR is measured by the size of its feedback logic as a Boolean circuit.

### 2.3 The cycle structure of FSRs

A binary sequence  $s$  is a map from  $\mathbb{Z}$  to  $\{0, 1\}$ . If there exists some  $\tau \in \mathbb{Z}$  such that  $s(t + \tau) = s(t)$  for any  $t \in \mathbb{Z}$ ,  $s$  is said to be *periodic* and the *period* of  $s$  is defined to be

$$\text{per}(s) = \min \{ \tau > 0 : s(t + \tau) = s(t) \text{ for all } t \in \mathbb{Z} \}.$$

Let  $f$  be an  $m$ -stage FSR. The following three statements are equivalent [3]: (i) The state transformation of  $f$  is bijective. (ii) Any sequence generated by  $f$  is periodic. (iii)  $f(x_0, x_1, \dots, x_m) = x_m \oplus g(x_1, x_2, \dots, x_{m-1}) \oplus x_0$  for some  $(m-1)$ -input Boolean function  $g$ . If any of (i)-(iii) holds,  $f$  is said to be *nonsingular*.

In the rest of this section we only consider nonsingular FSRs.

A sequence  $s$  of period  $m$  determines a cyclic sequence  $\theta(s) = [s(0), s(1), \dots, s(m-1)]$ . We call  $\theta(s)$  to be an  $m$ -cycle and also denote  $\text{per}(\theta(s)) = m$ . For the  $m$ -cycle  $\theta(s)$ , define the set

$$S_k(\theta(s)) = \{ (s(i), s((i+1) \bmod m), \dots, s((i+k-1) \bmod m)) \in \{0, 1\}^k : 0 \leq i < m \}.$$

Actually, any shift of a periodic sequence determines the same cycle, and  $\{s' : \theta(s') = \theta(s)\}$  is exactly the set of all shifts of  $s$ . Furthermore, if  $s \in G(f)$  for a  $k$ -stage FSR  $f$ , then each vector in  $S_k(\theta(s))$  plays as a unique initial state and hence determines a unique sequence in  $\{s' : \theta(s') = \theta(s)\}$ .

The *cycle structure* of an FSR  $f$ , denoted by **CycStr**( $f$ ), is  $\{\theta(s) : s \in G(f)\}$ .

Following this definition, we have the lemma below.

**Lemma 2.** *Let  $f$  and  $g$  be FSRs. Then  $g$  is a subFSR of  $f$  if and only if  $\text{CycStr}(g) \subset \text{CycStr}(f)$ .*

**Lemma 3.** *Let  $f$  be an  $m$ -stage FSR. Suppose  $\mathbf{c}, \mathbf{d} \in \text{CycStr}(f)$  (including  $\mathbf{c} = \mathbf{d}$ ),  $\mathbf{u} \in S_m(\mathbf{c})$  and  $\hat{\mathbf{u}} \in S_m(\mathbf{d})$ . Then  $\min(S_m(\mathbf{c}) \cup S_m(\mathbf{d})) < \min\{\mathbf{u}, \hat{\mathbf{u}}\}$  or  $\mathbf{u} \in \{\mathbf{0}^m, \mathbf{1}^m\}$ .*

*Proof.* Let  $F$  denote the state transformation of the FSR  $f$ . Then  $\{F(\mathbf{u}), F(\hat{\mathbf{u}})\} = \{\langle \mathbf{u}/2 \rangle, \langle \mathbf{u}/2 \rangle + 2^{m-1}\}$ , where  $\langle \mathbf{u}/2 \rangle = \max \{i \in \mathbb{Z} : i \leq \mathbf{u}/2\}$ .

Notice that  $F(\mathbf{u}) \in S_m(\mathbf{c})$ ,  $F(\hat{\mathbf{u}}) \in S_m(\mathbf{d})$  and  $\{\mathbf{u}, \hat{\mathbf{u}}\} = \{2\langle \mathbf{u}/2 \rangle, 2\langle \mathbf{u}/2 \rangle + 1\}$ . If  $\langle \mathbf{u}/2 \rangle > 0$ , then  $\langle \mathbf{u}/2 \rangle < \min\{\mathbf{u}, \hat{\mathbf{u}}\}$ , implying

$$\min(S_m(\mathbf{c}) \cup S_m(\mathbf{d})) \leq \min\{F(\mathbf{u}), F(\hat{\mathbf{u}})\} < \min\{\mathbf{u}, \hat{\mathbf{u}}\}.$$

If  $\langle \mathbf{u}/2 \rangle = 0$ , then  $\mathbf{u} \in \{\mathbf{0}^m, \mathbf{1}^m\}$ . □

**Lemma 4.** *Let  $\mathfrak{C}$  be a set of cycles. Then there exists an  $m$ -stage FSR  $f$  with  $\text{CycStr}(f) = \mathfrak{C}$  if and only if the following two conditions hold: (i)  $\sum_{\mathbf{c} \in \mathfrak{C}} \text{per}(\mathbf{c}) = 2^m$ ; (ii) The map  $\mathbf{v} \mapsto \lfloor \mathbf{v} \rfloor_m$  is injective on  $\bigcup_{\mathbf{c} \in \mathfrak{C}} S_{m+1}(\mathbf{c})$ .*

---

<sup>3</sup> Some theorists adopt the term “propositional directed acyclic graph(PDAG)”, and a PDAG is essentially the same as a Boolean circuit.

To prove Lemma 4, we use the following Lemma.

**Lemma 5.** *Let  $\mathfrak{C}$  be a set of finitely many cycles. Then the following three statements are equivalent: (i)  $|\bigcup_{c \in \mathfrak{C}} S_m(c)| = \sum_{c \in \mathfrak{C}} \text{per}(c)$ ; (ii) The map  $\mathbf{v} \mapsto [\mathbf{v}]_m$  is injective on  $\bigcup_{c \in \mathfrak{C}} S_{m+1}(c)$ ; (iii) The map  $\mathbf{v} \mapsto [\mathbf{v}]_m$  is injective on  $\bigcup_{c \in \mathfrak{C}} S_{m+1}(c)$ .*

*Proof.* First we prove that Statements (i) and (ii) are equivalent.

Let  $\mathfrak{C} = \{c_1, c_2, \dots, c_k\}$  and  $c_i = [c_{i,0}, c_{i,1}, \dots, c_{i,p_i-1}]$ ,  $1 \leq i \leq k$ , where  $p_i = \text{per}(c_i)$ . In this proof, a tuple  $(i, j)$  denotes a pair of integers satisfying  $1 \leq i \leq k$  and  $0 \leq j < p_i$ . Denote

$$\begin{aligned} \mathbf{x}_{i,j} &= (c_{i,(j+1) \bmod p_i}, c_{i,(j+2) \bmod p_i}, \dots, c_{i,(j+m) \bmod p_i}); \\ \mathbf{y}_{i,j} &= (c_{i,j}, c_{i,(j+1) \bmod p_i}, c_{i,(j+2) \bmod p_i}, \dots, c_{i,(j+m) \bmod p_i}). \end{aligned}$$

Notice  $\bigcup_{c \in \mathfrak{C}} S_m(c) = \bigcup_{i=1}^k \{\mathbf{x}_{i,j} : 0 \leq j < p_i\}$  and  $\bigcup_{c \in \mathfrak{C}} S_{m+1}(c) = \bigcup_{i=1}^k \{\mathbf{y}_{i,j} : 0 \leq j < p_i\}$ . It is sufficient to consider cases below.

- Case  $|\bigcup_{c \in \mathfrak{C}} S_m(c)| = \sum_{c \in \mathfrak{C}} \text{per}(c)$ . Then  $\mathbf{x}_{i,j} = \mathbf{x}_{i',j'}$  if and only if  $(i, j) = (i', j')$ . Since  $\mathbf{x}_{i,j} = [\mathbf{y}_{i,j}]_m$ ,  $\mathbf{y}_{i,j} = \mathbf{y}_{i',j'}$  occurs only if  $(i, j) = (i', j')$ . That is, the map  $\mathbf{y}_{i,j} \mapsto [\mathbf{y}_{i,j}]_m = \mathbf{x}_{i,j}$  is injective on  $\bigcup_{c \in \mathfrak{C}} S_{m+1}(c)$ .
- Case  $|\bigcup_{c \in \mathfrak{C}} S_m(c)| \neq \sum_{c \in \mathfrak{C}} \text{per}(c)$ . Then  $\mathbf{x}_{i_0,j_0} = \mathbf{x}_{i'_0,j'_0}$  for some  $(i_0, j_0) \neq (i'_0, j'_0)$ .

*Claim:* If  $\mathbf{x}_{i,j_0} = \mathbf{x}_{i',j'_0}$  for some  $(i, j_0) \neq (i', j'_0)$ , then there exists  $(i, j_1)$  and  $(i', j'_1)$  such that  $\mathbf{x}_{i,j_1} = \mathbf{x}_{i',j'_1}$  and  $\mathbf{y}_{i,j_1} \neq \mathbf{y}_{i',j'_1}$ .

*Proof of the claim.* Assume that this claim does not hold. Then for any  $(i, j_1)$  and  $(i', j'_1)$ , if  $\mathbf{x}_{i,j_1} = \mathbf{x}_{i',j'_1}$  then  $\mathbf{y}_{i,j_1} = \mathbf{y}_{i',j'_1}$ . Notice that  $\mathbf{y}_{i,j} = \mathbf{y}_{i',j'}$  implies  $\mathbf{x}_{i,(j-1) \bmod p_i} = \mathbf{x}_{i',(j'-1) \bmod p_{i'}}$ . Then  $\mathbf{x}_{i,(j_0-t) \bmod p_i} = \mathbf{x}_{i',(j'_0-t) \bmod p_{i'}}$  for any  $t \geq 0$ . Hence,  $c_i = c_{i'}$  and  $p_i \mid (j'_0 - j_0)$ , contradictory to  $(i, j_0) \neq (i', j'_0)$ . Therefore, our assumption is absurd and the claim is proved.

Following this claim, we assume  $\mathbf{x}_{i_0,j_0} = \mathbf{x}_{i'_0,j'_0}$  and  $\mathbf{y}_{i_0,j_0} \neq \mathbf{y}_{i'_0,j'_0}$  for some  $(i_0, j_0) \neq (i'_0, j'_0)$ . Thus, the map  $\mathbf{v} \mapsto [\mathbf{v}]_m$  is not injective on  $\bigcup_{c \in \mathfrak{C}} S_{m+1}(c)$ .

The proof of equivalence of Statements (i) and (iii) is similar and we omit it here.  $\square$

*Proof of Lemma 4.* By Lemma 5, it is sufficient to prove this statement:  $\mathbf{CycStr}(f) = \mathfrak{C}$  if and only if  $|\bigcup_{c \in \mathfrak{C}} S_m(c)| = \sum_{c \in \mathfrak{C}} \text{per}(c) = 2^m$ .

Suppose  $\mathfrak{C} = \mathbf{CycStr}(f)$  for some  $m$ -stage FSR  $f$ . Then for any  $c \in \mathfrak{C}$ , a vector in  $S_m(c)$  is exactly an initial state and uniquely determines a sequence in  $G(f)$ . Thus,  $\bigcup_{c \in \mathfrak{C}} S_m(c) = \{0, 1\}^k$  and  $|\bigcup_{c \in \mathfrak{C}} S_m(c)| = \sum_{c \in \mathfrak{C}} \text{per}(c)$ .

Suppose  $|\bigcup_{c \in \mathfrak{C}} S_m(c)| = \sum_{c \in \mathfrak{C}} \text{per}(c) = 2^m$ . Then  $\bigcup_{c \in \mathfrak{C}} S_m(c) = \{0, 1\}^m$ . Define an  $m$ -input Boolean function  $f_1$  as follows. By Lemma 5, for any  $\mathbf{v} = (a_0, a_1, \dots, a_{m-1}) \in \{0, 1\}^m$ , there exists uniquely  $b \in \{0, 1\}$  such that  $(a_0, a_1, \dots, a_{m-1}, b) \in \bigcup_{c \in \mathfrak{C}} S_{m+1}(c)$ . We define  $f_1(\mathbf{v}) = b$ . Immediately,  $\mathfrak{C}$  is the cycle structure of an FSR whose feedback logic is logically equivalent to  $f_1$ .  $\square$

**Lemma 6.** *Let  $f$  be an  $m$ -stage FSR and  $F$  the state transformation of  $f$ . Let  $c \in \mathbf{CycStr}(f)$  and  $\text{per}(c) = p$ . Then for any  $\mathbf{v} \in S_m(c)$ ,  $\min\{i > 0 : F^i(\mathbf{v}) = \mathbf{v}\} = p$  and  $S_m(c) = \{\mathbf{v}, F(\mathbf{v}), \dots, F^{p-1}(\mathbf{v})\}$ .*

*Proof.* Let  $\mathbf{v} \in S_m(c)$  and  $q = \min\{i > 0 : F^i(\mathbf{v}) = \mathbf{v}\}$ . Clearly,  $q \leq p$ . Then

$$c = [[\mathbf{v}]_1, [F(\mathbf{v})]_1, \dots, [F^{q-1}(\mathbf{v})]_1],$$

and  $q = \text{per}(c) = p$ . Because  $\{F^i(\mathbf{v}) : i \in \mathbb{Z}\} \subseteq S_m(c)$  and  $|S_m(c)| \leq \text{per}(c)$ , we conclude that  $|S_m(c)| = p$  and  $S_m(c) = \{\mathbf{v}, F(\mathbf{v}), \dots, F^{p-1}(\mathbf{v})\}$  is a set of  $p$  vectors in  $\{0, 1\}^m$ .  $\square$

**Lemma 7.** Let  $g(x_0, x_1, \dots, x_m)$  be an  $m$ -stage FSR and

$$f(x_0, x_1, \dots, x_m) = g(x_0, x_1, \dots, x_m) \oplus f_3(x_1, x_2, \dots, x_{m-1}),$$

where  $f_3$  is an  $(m-1)$ -input Boolean logic. Let  $\lambda : \{0, 1\}^m \rightarrow \{0, 1\}$  be a map satisfying

$$\begin{cases} |\{\mathbf{v} \in S_m(\mathbf{c}) : \lambda(\mathbf{v}) = 1\}| \leq 1 \text{ for any } \mathbf{c} \in \mathbf{CycStr}(g); \\ \lambda(\mathbf{v}) \cdot \lambda(\widehat{\mathbf{v}}) = 0 \text{ for any } \mathbf{v} \in \{0, 1\}^m; \\ \text{For any } \mathbf{u} \in \{0, 1\}^{m-1} \text{ with } f_3(\mathbf{u}) = 1, \text{ there exists } b \in \{0, 1\} \text{ satisfying } \lambda(b \parallel \mathbf{u}) = 1. \end{cases} \quad (2)$$

A directed graph  $D_g^f$  is defined as follows: the set of vertices is  $\mathbf{CycStr}(g)$ , and an arc is incident from  $\mathbf{c}_1$  to  $\mathbf{c}_2$  if and only if

$$\{\mathbf{v} \in S_m(\mathbf{c}_1) : f_3(\lfloor \mathbf{v} \rfloor_{m-1}) = 1, \lambda(\mathbf{v}) = 1, \widehat{\mathbf{v}} \in S_m(\mathbf{c}_2)\} \neq \emptyset.$$

If  $D_g^f$  is acyclic, then the following two statements hold: (i) Any  $\mathbf{d} \in \mathbf{CycStr}(f)$  is joined by all cycles in a weakly connected component<sup>4</sup>  $\mathfrak{C}$  of  $D_g^f$  and  $S_m(\mathbf{d}) = \bigcup_{\mathbf{c} \in \mathfrak{C}} S_m(\mathbf{c})$ . (ii) If  $h$  is a subFSR of  $f$ , then  $\mathbf{CycStr}(h) \subset \mathbf{CycStr}(g)$ .

*Proof.* Statement (i) of this lemma follows from the idea of the cycle joining method [3], and we leave its proof in Appendix 6.1. Below we prove Statement (ii) of this lemma.

By Lemmas 2 and 4, it is sufficient to prove this statement: if  $\mathfrak{C} \subset \mathbf{CycStr}(f)$  and  $\mathfrak{C} \not\subset \mathbf{CycStr}(g)$ , then for any  $1 \leq k < m$ , the map  $\mathbf{v} \mapsto \lfloor \mathbf{v} \rfloor_k$  is not injective on  $\bigcup_{\mathbf{c} \in \mathfrak{C}} S_{k+1}(\mathbf{c})$ . Suppose  $\mathbf{d} \in \mathfrak{C} \setminus \mathbf{CycStr}(g)$ . As proved in Statement (i),  $\mathbf{d}$  is joined by the cycles composing a weakly connected component  $\mathfrak{D}$  of the graph  $D_g^f$ . Since  $\mathfrak{D} \subset \mathbf{CycStr}(g)$  and  $\mathbf{d} \notin \mathbf{CycStr}(g)$ , we have  $|\mathfrak{D}| > 1$ . Hence, by Statement (i) and the definition of  $D_g^f$ , there exists  $\mathbf{v} \in \{0, 1\}^m$  satisfying  $\{\mathbf{v}, \widehat{\mathbf{v}}\} \subset S_m(\mathbf{d})$ . Then for any  $1 \leq k < m$ ,  $\lfloor \mathbf{v} \rfloor_{k+1}, \lfloor \widehat{\mathbf{v}} \rfloor_{k+1} \in S_{k+1}(\mathbf{d})$  satisfy  $\lfloor \mathbf{v} \rfloor_{k+1} \neq \lfloor \widehat{\mathbf{v}} \rfloor_{k+1}$  and  $\lfloor \lfloor \mathbf{v} \rfloor_{k+1} \rfloor_k = \lfloor \lfloor \widehat{\mathbf{v}} \rfloor_{k+1} \rfloor_k$ . Therefore, the map  $\mathbf{v} \mapsto \lfloor \mathbf{v} \rfloor_k$  is not injective on  $S_{k+1}(\mathbf{d})$ , and hence is not injective on  $\bigcup_{\mathbf{c} \in \mathfrak{C}} S_{k+1}(\mathbf{c})$ .  $\square$

Given an  $m$ -cycle  $\mathbf{c} = [b_0, b_1, \dots, b_m]$ , let  $\bar{\mathbf{c}}$  denote the cycle  $[b_0 \oplus 1, b_1 \oplus 1, \dots, b_m \oplus 1]$ .

The cycle structure of LFSRs is well understood.

**Lemma 8.** Let  $n = 3^k$ ,  $0 \leq k \in \mathbb{Z}$ . Let  $p_0(x) = x^{2n} \oplus x^n \oplus 1$ ,  $p_1(x) = (x \oplus 1) \cdot p_0(x)$ , and  $p_2(x) = x^{4n} \oplus x^{2n} \oplus 1$  be polynomials over the binary field  $\mathbb{F}_2$ . Then  $p_0$  is irreducible over  $\mathbb{F}_2$  and

$$\begin{aligned} \mathbf{CycStr}(p_0) &= \left\{ [0], \beta_1, \beta_2, \dots, \beta_{\frac{2^{2n}-1}{3n}} \right\}, \\ \mathbf{CycStr}(p_1) &= \left\{ [0], \beta_1, \beta_2, \dots, \beta_{\frac{2^{2n}-1}{3n}}, [1], \bar{\beta}_1, \bar{\beta}_2, \dots, \bar{\beta}_{\frac{2^{2n}-1}{3n}} \right\}, \\ \mathbf{CycStr}(p_2) &= \left\{ [0], \beta_1, \beta_2, \dots, \beta_{\frac{2^{2n}-1}{3n}}, \gamma_1, \gamma_2, \dots, \gamma_{\frac{2^{4n}-2^{2n}}{6n}} \right\}, \end{aligned}$$

where  $\text{per}(\beta_i) = \text{per}(\bar{\beta}_i) = 3n$  for  $1 \leq i \leq \frac{2^{2n}-1}{3n}$ , and  $\text{per}(\gamma_i) = 6n$  for  $1 \leq i \leq \frac{2^{4n}-2^{2n}}{6n}$ .

*Proof.* Since  $p_0(x) \cdot (x^{3^k} \oplus 1) = x^{3^{k+1}} \oplus 1$  and  $\gcd(p_0, x^{3^k} \oplus 1) = 1$ , the roots of  $p_0$  are exactly primitive  $3^{k+1}$ -th roots of unity. Thus,  $p_0$  is irreducible and  $\min\{0 < t \in \mathbb{Z} : p_0 \mid (x^t - 1)\} = 3n$  is the order of any primitive  $3^{k+1}$ -th root of unity in the multiplicative group of the finite field  $\mathbb{F}_2[x]/(p_0(x))$ .

The rest of this lemma directly follows from [7, Theorem 8.53, 8.55, 8.63].  $\square$

<sup>4</sup> Let  $D$  be a directed graph with its set of vertices  $V$ . An undirected graph  $H$  is obtained by taking each arc of  $D$  as an edge of  $H$ . The weakly connected component(s) is(are) the connected component(s) of  $H$ . Formally, define a binary relation

$$R = \{(a, b) \in V \times V : \text{there is an arc incident from } a \text{ to } b \text{ or there is an arc incident from } b \text{ to } a\},$$

and then a weakly connected component of  $D$  is an equivalence class w.r.t. the equivalence closure of  $R$ .

### 3 NP-hardness of deciding irreducible FSRs

Below Algorithm 1 transforms a given Boolean circuit to an FSR.

In the rest of this section, we use notations  $f_0$ ,  $f_3$  and  $f$  defined in Algorithm 1.

Clearly,  $f$  is a nonsingular FSR.

Following Algorithm 1, the Boolean circuit  $f_3$  is described with Figures 3, 4, 5, 6 and 7. To ease our presentation, from now on we also use operations with finite fan-in and fan-out for sketching a Boolean circuit. For example, as  $x \oplus y = ((\neg x) \wedge y) \vee ((\neg y) \wedge x)$ , we allow XOR( $\oplus$ ), logically equivalent to a subcircuit consisting of five gates. In Figures 3, 4, 5 and 6, the operation “ $\stackrel{?}{=}$ ” decides whether two  $4n$ -bit inputs are

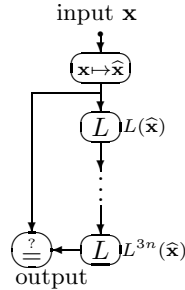


Figure 3: A diagram of the subcircuit CP

equal or not. In Figures 4 and 5, the operation “min” computes the minimum of two  $4n$ -bit integers.

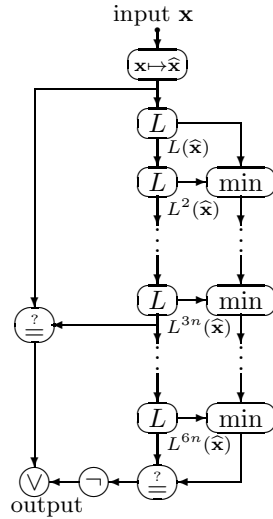


Figure 4: A diagram of the subcircuit CMP

**Lemma 9.** *Let  $f_1$  be the feedback logic of the FSR  $f$  given by Algorithm 1. Then  $\mathbf{SIZE}(f_1) < 37908 \cdot \mathbf{SIZE}(f_0)^4$  and Algorithm 1 is polynomial-time computable.*

*Proof.* The operation  $\mathbf{x} \mapsto \hat{\mathbf{x}}$  uses one NOT gate on  $[\mathbf{x}]_1$ . Given the input  $(x_0, x_1, \dots, x_{4n-1})$  and  $(y_0, y_1, \dots, y_{4n-1})$ , the operation “ $\stackrel{?}{=}$ ” outputs  $\neg((x_0 \oplus y_0) \vee (x_1 \oplus y_1) \vee \dots \vee (x_{4n-1} \oplus y_{4n-1}))$  and costs at most  $24n$  gates. The

---

**Algorithm 1** Transforming a Boolean circuit to an FSR
 

---

**Input:** An  $r$ -input Boolean circuit  $f_0$ .

**Output:** A  $4n$ -stage FSR  $f$ , where  $k = \min \{i \in \mathbb{Z} : i \geq \log_3(r/2)\}$  and  $n = 3^k$ .

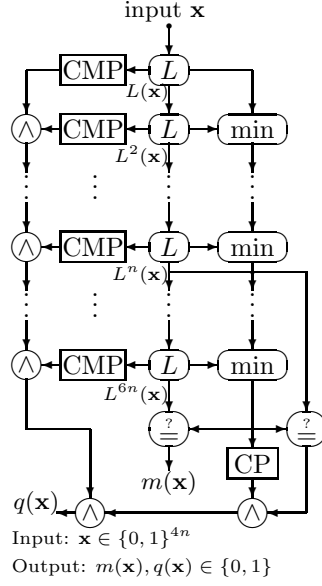
```

1: {Construct a  $(4n - 1)$ -input Boolean circuit  $f_3$  with its pseudocode in Lines 2-37. In the rest of this
   section,  $L$  denotes the state transformation of the LFSR  $x^{4n} \oplus x^{2n} \oplus 1$ . }
2: Let  $\mathbf{x} \in \{0, 1\}^{4n-1}$  be the input of  $f_3$ .
3: Let  $\mathbf{u}_0 = 0 \parallel \mathbf{x}$  and  $\mathbf{v}_0 = 1 \parallel \mathbf{x}$ .
4: for  $i = 1$  to  $6n$  do
5:    $\mathbf{u}_i = L(\mathbf{u}_{i-1})$  and  $\mathbf{v}_i = L(\mathbf{v}_{i-1})$ .
6:    $a_i = f_0(\lfloor \mathbf{u}_i \rfloor_r)$  and  $b_i = f_0(\lfloor \mathbf{v}_i \rfloor_r)$ .
7:   if  $L^{3n}(\widehat{\mathbf{u}}_i) = \widehat{\mathbf{u}}_i$  or  $L^{6n}(\widehat{\mathbf{u}}_i) \neq \min \{L^j(\widehat{\mathbf{u}}_i) : 1 \leq j \leq 6n\}$  then
8:      $c_i = 1$ .
9:   else
10:     $c_i = 0$ .
11:   end if
12:   if  $L^{3n}(\widehat{\mathbf{v}}_i) = \widehat{\mathbf{v}}_i$  or  $L^{6n}(\widehat{\mathbf{v}}_i) \neq \min \{L^j(\widehat{\mathbf{v}}_i) : 1 \leq j \leq 6n\}$  then
13:      $d_i = 1$ .
14:   else
15:      $d_i = 0$ .
16:   end if
17: end for
18:  $\mathbf{u}_{\min} = \min \{\mathbf{u}_i : 1 \leq i \leq 6n\}$  and  $\mathbf{v}_{\min} = \min \{\mathbf{v}_i : 1 \leq i \leq 6n\}$ .
19: if  $c_1 \wedge c_2 \wedge \dots \wedge c_{6n} = 1$  and  $\mathbf{u}_n = \mathbf{u}_{\min}$  and  $L^{3n}(\widehat{\mathbf{u}}_{\min}) = \widehat{\mathbf{u}}_{\min}$  then
20:    $q(\mathbf{u}_0) = 1$ .
21: else
22:    $q(\mathbf{u}_0) = 0$ .
23: end if
24: if  $d_1 \wedge d_2 \wedge \dots \wedge d_{6n} = 1$  and  $\mathbf{v}_n = \mathbf{v}_{\min}$  and  $L^{3n}(\widehat{\mathbf{v}}_{\min}) = \widehat{\mathbf{v}}_{\min}$  then
25:    $q(\mathbf{v}_0) = 1$ .
26: else
27:    $q(\mathbf{v}_0) = 0$ .
28: end if
29: if  $\mathbf{u}_0 = \mathbf{u}_{3n}$  and  $\mathbf{u}_{6n} = \mathbf{u}_{\min}$  and  $a_1 \vee a_2 \vee \dots \vee a_{6n} = 1$  then
30:   The Boolean circuit  $f_3$  returns 1.
31: else if  $\mathbf{v}_0 = \mathbf{v}_{3n}$  and  $\mathbf{v}_{6n} = \mathbf{v}_{\min}$  and  $b_1 \vee b_2 \vee \dots \vee b_{6n} = 1$  then
32:   The Boolean circuit  $f_3$  returns 1.
33: else if  $\mathbf{u}_0 \neq \mathbf{u}_{3n}$  and  $\mathbf{v}_0 \neq \mathbf{v}_{3n}$  and  $(\mathbf{u}_{6n} = \mathbf{u}_{\min}$  or  $\mathbf{v}_{6n} = \mathbf{v}_{\min}$  or  $q(\mathbf{u}_0) = 1$  or  $q(\mathbf{v}_0) = 1)$  then
34:   The Boolean circuit  $f_3$  returns 1.
35: else
36:   The Boolean circuit  $f_3$  returns 0.
37: end if
38: return the FSR  $f(x_0, \dots, x_{4n}) = x_{4n} \oplus x_{2n} \oplus x_0 \oplus f_3(x_1, x_2, \dots, x_{4n-1})$ .

```

---





The subcircuits CP and CMP are given in Figures 3 and 4, respectively.

Figure 5: A diagram of the subcircuit MQ

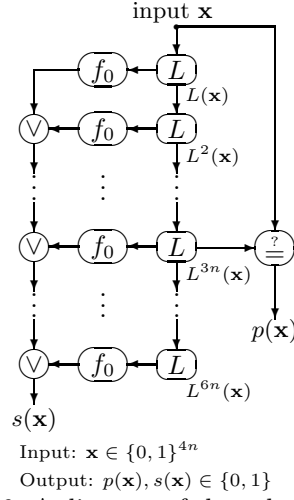
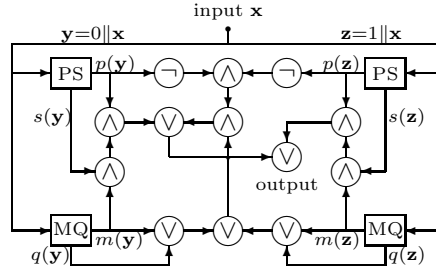


Figure 6: A diagram of the subcircuit PS



The subcircuits MQ and PS are given in Figures 5 and 6, respectively.

Figure 7: A diagram of the Boolean circuit  $f_3$

state transformation  $L$  is performed by one XOR gate, i.e., 5 gates. By Appendix 6.2, the operation “min” uses  $104n^2 + 66n - 22$  gates.

Noticing  $r \leq 2n \leq 3r - 1$ ,  $r \leq \mathbf{SIZE}(f_0)$  and

$$f_1(x_0, \dots, x_{4n-1}) = x_0 \oplus x_{2n} \oplus f_3(x_1, x_2, \dots, x_{4n-1}),$$

we count gates in Figure 7 and obtain

$$\begin{aligned} \mathbf{SIZE}(f_1) &= 11 + \mathbf{SIZE}(f_3) \\ &= 12n \cdot \mathbf{SIZE}(f_0) + 7488n^4 + 4752n^3 - 856n^2 + 274n + 69 \\ &< 37908 \cdot \mathbf{SIZE}(f_0)^4. \end{aligned}$$

The Boolean circuit  $f_0$  has  $\mathbf{SIZE}(f_0)$  vertices and less than  $2 \cdot \mathbf{SIZE}(f_0)$  arcs; The feedback logic  $f_1$  has at most  $37908 \cdot \mathbf{SIZE}(f_0)^4$  vertices and at most  $75816 \cdot \mathbf{SIZE}(f_0)^4$  arcs. The FSR  $f$  uses  $f_0$  and basic polynomial-time computable operations for at most  $37908 \cdot \mathbf{SIZE}(f_0)^4$  times and its main architecture is given by Figures 3, 4, 5, 6 and 7. Therefore, Algorithm 1 is polynomial-time computable.  $\square$

In the rest of this section,  $n$  is as given in Algorithm 1,  $p_0$  and  $p_2$  are the polynomials as defined in Lemma 8, we also denote  $\mathfrak{C}_{6n} = \mathbf{CycStr}(p_2) \setminus \mathbf{CycStr}(p_0)$ .

**Lemma 10.** *Let  $\mathbf{v} \in S_{4n}(\beta)$ , where  $\beta \in \mathbf{CycStr}(p_0)$ . Then  $\widehat{\mathbf{v}} \in S_{4n}(\gamma)$  for some  $\gamma \in \mathfrak{C}_{6n}$ .*

*Proof.* Suppose  $\widehat{\mathbf{v}} \in S_{4n}(\gamma)$  for some  $\gamma \in \mathbf{CycStr}(p_0)$ . By Lemmas 6 and 8,  $L^{3n}(\widehat{\mathbf{v}}) = \widehat{\mathbf{v}}$  and  $L^{3n}(\mathbf{v}) = \mathbf{v}$ . Since  $L$  is a linear transformation and  $\iota^{4n} = \mathbf{v} \oplus \widehat{\mathbf{v}}$ , we have  $L^{3n}(\iota^{4n}) = \iota^{4n}$ , contradictory to  $L^{3n}(\iota^{4n}) = (\mathbf{0}^n \mathbf{10}^{2n-1} \mathbf{10}^{n-1})$ , where this vector is written without commas between bits. Therefore, the supposition above is absurd and  $\gamma \in \mathfrak{C}_{6n}$ .  $\square$

Because any  $\mathbf{v} \in \{0, 1\}^{4n}$ , as an initial state of the  $4n$ -stage LFSR  $p_2$ , determines a unique cycle, in the rest of this section we denote  $\xi(\mathbf{v}) = \mathbf{c} \in \mathbf{CycStr}(p_2)$  such that  $\mathbf{v} \in S_{4n}(\mathbf{c})$ .

**Lemma 11.** *Let*

$$\begin{aligned} \mathfrak{D} = \{ \mathbf{c} \in \mathbf{CycStr}(p_2) : \xi(\min S_{4n}(\mathbf{c}) \oplus \iota^{4n}) \in \mathbf{CycStr}(p_0), \\ \{ \mathbf{v} \in S_{4n}(\mathbf{c}) : \xi(\widehat{\mathbf{v}}) \in \mathfrak{C}_{6n} \text{ and } \widehat{\mathbf{v}} = \min S_{4n}(\xi(\widehat{\mathbf{v}})) \} = \emptyset \} \end{aligned}$$

and define a map  $\rho : \mathbf{CycStr}(p_2) \rightarrow \{0, 1\}^{4n}$  as

$$\rho(\mathbf{c}) = \begin{cases} \min S_{4n}(\mathbf{c}), & \text{if } \mathbf{c} \in \mathbf{CycStr}(p_2) \setminus \mathfrak{D}; \\ L^{5n}(\min S_{4n}(\mathbf{c})), & \text{if } \mathbf{c} \in \mathfrak{D}. \end{cases}$$

Then the following two statements hold: (i)  $\mathfrak{D} \subset \mathfrak{C}_{6n}$  and for any  $\mathbf{c} \in \mathfrak{D}$ ,  $\xi(\widehat{\rho(\mathbf{c})}) \in \mathfrak{C}_{6n} \setminus \mathfrak{D}$ . (ii) If  $\mathbf{c} \in \mathbf{CycStr}(p_2)$  and  $\widehat{\rho(\mathbf{c})} \in \{ \rho(\mathbf{e}) : \mathbf{e} \in \mathbf{CycStr}(p_2) \}$ , then  $\mathbf{c} \in \{[0], \xi(\iota^{4n})\}$ .

*Proof.* For convenience in this proof we may write a cycle or vector without commas between its bits.

*Claim:* If  $\mathbf{c} \in \mathbf{CycStr}(p_2)$  satisfies  $\xi(\min S_{4n}(\mathbf{c}) \oplus \iota^{4n}) \in \mathbf{CycStr}(p_0)$ , then  $\mathbf{c} = [\mathbf{u}_0 \mathbf{u}_1 \mathbf{u}_2 \mathbf{u}_3 \mathbf{u}_4 \mathbf{u}_5]$ , where  $\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2 \in \{0, 1\}^{n-1}$ ,  $\mathbf{u}_2 = \mathbf{u}_0 \oplus \mathbf{u}_1$  and  $(\mathbf{1u}_0 \mathbf{0u}_1 \mathbf{0u}_2 \mathbf{0u}_3) = \min S_{4n}(\mathbf{c})$ .

*Proof of the claim.* By Lemma 10,  $\mathbf{c} \in \mathfrak{C}_{6n}$ . Denote  $\mathbf{c} = [a_0 \mathbf{u}_0 a_1 \mathbf{u}_1 a_2 \mathbf{u}_2 a_3 \mathbf{u}_3 a_4 \mathbf{u}_4 a_5 \mathbf{u}_5]$ , where

$$\begin{cases} a_i \in \{0, 1\}, 0 \leq i \leq 5; \\ \mathbf{u}_i \in \{0, 1\}^{n-1}, 0 \leq i \leq 5; \\ (a_0 \mathbf{u}_0 a_1 \mathbf{u}_1 a_2 \mathbf{u}_2 a_3 \mathbf{u}_3) = \min S_{4n}(\mathbf{c}). \end{cases}$$

Notice  $\xi(\iota^{4n}) = [1\mathbf{0}^{4n-1}1\mathbf{0}^{2n-1}]$ . Then  $\overline{a_0}\mathbf{u}_0a_1\mathbf{u}_1a_2\mathbf{u}_2a_3\mathbf{u}_3\overline{a_4}\mathbf{u}_4a_5\mathbf{u}_5$  is concatenation of a same cycle in  $\mathbf{CycStr}(p_0)$ , implying where  $a_2 = a_0 \oplus a_1 \oplus 1$  and  $\mathbf{u}_2 = \mathbf{u}_0 \oplus \mathbf{u}_1$ . By Lemma 8,

$$\mathbf{c} = [a_0\mathbf{u}_0a_1\mathbf{u}_1a_2\mathbf{u}_2\overline{a_0}\mathbf{u}_0\overline{a_1}\mathbf{u}_1a_2\mathbf{u}_2].$$

By

$$(a_0\mathbf{u}_0a_1\mathbf{u}_1a_2\mathbf{u}_2\overline{a_0}\mathbf{u}_0) \leq (\overline{a_0}\mathbf{u}_0\overline{a_1}\mathbf{u}_1a_2\mathbf{u}_2a_0\mathbf{u}_0),$$

we have  $a_0 = 1$ . By

$$(a_0\mathbf{u}_0a_1\mathbf{u}_1a_2\mathbf{u}_2\overline{a_0}\mathbf{u}_0) \leq (\mathbf{u}_0a_1\mathbf{u}_1a_2\mathbf{u}_2\overline{a_0}\mathbf{u}_0\overline{a_1}),$$

we have  $a_1 = 0$ . Then  $a_2 = 0$ . The proof of this claim is complete.

For a  $kn$ -cycle  $\mathbf{c} = [b_0, b_1, \dots, b_{kn-1}]$ , we call

$$(b_i, b_{(i+n) \bmod kn}, b_{(i+2n) \bmod kn}, \dots, b_{(i+(k-1)n} \bmod kn))$$

an  $n$ -sampling of  $\mathbf{c}$ ,  $0 \leq i < kn$ .

Choose any  $\mathbf{c} \in \mathfrak{D}$ . Because of the claim above, let  $\mathbf{c} = [1\mathbf{u}_00\mathbf{u}_10\mathbf{u}_20\mathbf{u}_01\mathbf{u}_10\mathbf{u}_2]$ , where  $\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2 \in \{0, 1\}^{n-1}$ ,  $\mathbf{u}_2 = \mathbf{u}_0 \oplus \mathbf{u}_1$  and  $(1\mathbf{u}_00\mathbf{u}_10\mathbf{u}_20\mathbf{u}_0) = \min S_{4n}(\mathbf{c})$ . Then

$$\widehat{\rho(\mathbf{c})} = \iota^{4n} \oplus L^{5n}(\min S_{4n}(\mathbf{c})) = (1\mathbf{u}_21\mathbf{u}_00\mathbf{u}_10\mathbf{u}_2)$$

and hence

$$\xi(\widehat{\rho(\mathbf{c})}) = [1\mathbf{u}_21\mathbf{u}_00\mathbf{u}_10\mathbf{u}_21\mathbf{u}_01\mathbf{u}_1].$$

First,  $3n \nmid \text{per}(\xi(\widehat{\rho(\mathbf{c})}))$ . By Lemma 8,  $\xi(\widehat{\rho(\mathbf{c})}) \in \mathfrak{C}_{6n}$ . Second, as shown in the claim above, there is an  $n$ -sampling (100010) of any cycle in  $\mathfrak{D}$ , while (100010) is not an  $n$ -sampling of  $\xi(\widehat{\rho(\mathbf{c})})$ . Hence,  $\xi(\widehat{\rho(\mathbf{c})}) \notin \mathfrak{D}$ . By Lemma 10,  $\mathbf{c} \notin \mathbf{CycStr}(p_0)$ . Till now Statement (i) of this lemma is proved.

Now we prove Statement (ii) of this lemma.

Denote  $\mathbf{v}_0 = (01\mathbf{0}^{4n-2})$ . Then  $\xi(\widehat{\mathbf{v}_0}) = [11\mathbf{0}^{4n-2}11\mathbf{0}^{2n-2}]$ . By Lemma 8,  $\xi(\widehat{\mathbf{v}_0}) \in \mathfrak{C}_{6n}$ . Seeing  $\widehat{\mathbf{v}_0} = \min S_{4n}(\xi(\widehat{\mathbf{v}_0}))$  and  $\mathbf{v}_0 \in S_{4n}(\xi(\iota^{4n}))$ , we have  $\xi(\iota^{4n}) \notin \mathfrak{D}$  and  $\iota^{4n} = \rho(\xi(\iota^{4n}))$ .

Denote  $V_c = \{\rho(\mathbf{e}) : \mathbf{e} \in \mathbf{CycStr}(p_2)\}$ . Notice that  $\rho(\mathbf{c}) \in S_{4n}(\mathbf{c})$ ,  $\mathbf{c} \in \mathbf{CycStr}(p_2)$ . It is sufficient to consider the following cases.

1. If  $\mathbf{c} \in \mathfrak{D}$ , by Statement (i),  $\xi(\widehat{\rho(\mathbf{c})}) \in \mathfrak{C}_{6n} \setminus \mathfrak{D}$ . By the definition of  $\mathfrak{D}$ ,

$$\widehat{\rho(\mathbf{c})} \neq \min S_{4n}(\xi(\widehat{\rho(\mathbf{c})})) = \rho(\xi(\widehat{\rho(\mathbf{c})}))$$

and hence  $\widehat{\rho(\mathbf{c})} \notin V_c$ .

2. If  $\xi(\iota^{4n}) \neq \mathbf{c} \in \mathfrak{C}_{6n} \setminus \mathfrak{D}$ , then  $\rho(\mathbf{c}) = \min S_{4n}(\mathbf{c}) \notin \{\mathbf{0}^{4n}, \iota^{4n}\}$ . By the definition of  $\mathfrak{D}$ ,  $\xi(\widehat{\rho(\mathbf{c})}) \notin \mathfrak{D}$ , yielding  $\rho(\xi(\widehat{\rho(\mathbf{c})})) = \min S_{4n}(\xi(\widehat{\rho(\mathbf{c})}))$ . By Lemma 3,  $\widehat{\rho(\mathbf{c})} \neq \min S_{4n}(\xi(\widehat{\rho(\mathbf{c})}))$  and hence  $\widehat{\rho(\mathbf{c})} \notin V_c$ .

3. If  $[0] \neq \mathbf{c} \in \mathbf{CycStr}(p_0)$  and  $\xi(\widehat{\rho(\mathbf{c})}) \notin \mathfrak{D}$ , then similar to Case (2), we also get  $\widehat{\rho(\mathbf{c})} \notin V_c$ .

4. If  $\mathbf{c} \in \mathbf{CycStr}(p_0)$  and  $\xi(\widehat{\rho(\mathbf{c})}) \in \mathfrak{D}$ , then by the proved Statement (i) of this lemma,

$$\mathbf{c} \neq \xi(\rho(\xi(\widehat{\rho(\mathbf{c})}))) \oplus \iota^{4n} \in \mathfrak{C}_{6n}.$$

Because  $\xi(\rho(\mathbf{e})) = \mathbf{e}$  for any  $\mathbf{e} \in \mathbf{CycStr}(p_2)$ , we have  $\widehat{\rho(\mathbf{c})} \neq \rho(\xi(\widehat{\rho(\mathbf{c})}))$ , yielding  $\widehat{\rho(\mathbf{c})} \notin V_c$ .

5. Besides, consider  $\mathbf{c} \in \{[0], \xi(\iota^{4n})\}$ . We have  $\widehat{\rho([0])} = \iota^{4n} = \rho(\xi(\iota^{4n}))$  since  $\xi(\iota^{4n}) \in \mathfrak{C}_{6n} \setminus \mathfrak{D}$ .

Till now all cases are listed and Statement (ii) of this lemma holds.  $\square$

**Lemma 12.** Let  $\rho$  be given in Lemma 11. Let the map  $\lambda : \{0, 1\}^{4n} \rightarrow \{0, 1\}$  be defined as

$$\lambda(\mathbf{v}) = \begin{cases} 1, & \text{if } \mathbf{v} \in \{\rho(\mathbf{c}) : \mathbf{c} \in \mathbf{CycStr}(p_2)\} \text{ and } \xi(\widehat{\mathbf{v}}) \in \mathfrak{C}_{6n}; \\ 0, & \text{otherwise.} \end{cases}$$

Let  $D_{p_2}^f$  be the graph defined as in Lemma 7 (Recall that  $f$  and  $f_3$  are given in Algorithm 1). Then the following statements hold: (i) Statements (i) and (ii) of Lemma 7 hold, where  $g$  in Lemma 7 is the LFSR  $p_2$ . (ii) Each  $\mathbf{c} \in \mathfrak{C}_{6n}$  is not an isolated vertex in  $D_{p_2}^f$ . (iii) Every  $\mathbf{c} \in \mathbf{CycStr}(p_0)$  is an isolated vertex in  $D_{p_2}^f$  if and only if  $f_0$  is unsatisfiable.

*Proof.* Since  $\rho(\mathbf{c}) \in S_{4n}(\mathbf{c})$  for any  $\mathbf{c} \in \mathbf{CycStr}(p_2)$ , we have

$$|\{\mathbf{v} \in S_{4n}(\mathbf{c}) : \lambda(\mathbf{v}) = 1\}| \leq |\{\rho(\mathbf{c})\}| = 1.$$

Following from Statement (ii) of Lemma 11 and  $\lambda(\iota^{4n}) = 0$ , we have  $\lambda(\mathbf{v}) \cdot \lambda(\widehat{\mathbf{v}}) = 0$  for any  $\mathbf{v} \in \{0, 1\}^{4n}$ .

Use  $\mathfrak{D}$  defined in Lemma 11.

Let  $q(\mathbf{u}_0)$ ,  $q(\mathbf{v}_0)$ ,  $\mathbf{u}_i$  and  $\mathbf{v}_i$  be as in Algorithm 1,  $0 \leq i \leq 6n$ . Denote  $\mathbf{e}_0 = \xi(\mathbf{u}_0)$  and  $\mathbf{e}_1 = \xi(\mathbf{v}_0)$ . By Lemmas 6 and 8,  $S_{4n}(\mathbf{e}_0) = \{\mathbf{u}_i : 1 \leq i \leq 6n\}$ ;  $S_{4n}(\mathbf{e}_1) = \{\mathbf{v}_i : 1 \leq i \leq 6n\}$ ;  $\mathbf{u}_0 = \mathbf{u}_{6n}$ ;  $\mathbf{v}_0 = \mathbf{v}_{6n}$ ;  $\mathbf{u}_0 = \mathbf{u}_{3n}$  (resp.  $\mathbf{v}_0 = \mathbf{v}_{3n}$ ) if and only if  $\mathbf{e}_0 \in \mathbf{CycStr}(p_0)$  (resp.  $\mathbf{e}_1 \in \mathbf{CycStr}(p_0)$ );  $L^{3n}(\widehat{\mathbf{u}}_i) = \widehat{\mathbf{u}}_i$  (resp.  $L^{3n}(\widehat{\mathbf{v}}_i) = \widehat{\mathbf{v}}_i$ ) if and only if  $\xi(\widehat{\mathbf{u}}_i) \in \mathbf{CycStr}(p_0)$  (resp.  $\xi(\widehat{\mathbf{v}}_i) \in \mathbf{CycStr}(p_0)$ );  $L^{6n}(\widehat{\mathbf{u}}_i) \neq \min\{L^j(\widehat{\mathbf{u}}_i) : 1 \leq j \leq 6n\}$  (resp.  $L^{6n}(\widehat{\mathbf{v}}_i) \neq \min\{L^j(\widehat{\mathbf{v}}_i) : 1 \leq j \leq 6n\}$ ) if and only if  $\widehat{\mathbf{u}}_i \neq \min S_{4n}(\xi(\widehat{\mathbf{u}}_i))$  (resp.  $\widehat{\mathbf{v}}_i \neq \min S_{4n}(\xi(\widehat{\mathbf{v}}_i))$ );  $\mathbf{u}_n = \mathbf{u}_{\min}$  (resp.  $\mathbf{v}_n = \mathbf{v}_{\min}$ ) if and only if  $\mathbf{u}_0 = L^{5n}(\min S_{4n}(\mathbf{e}_0))$  (resp.  $\mathbf{v}_0 = L^{5n}(\min S_{4n}(\mathbf{e}_1))$ );  $L^{3n}(\widehat{\mathbf{u}}_{\min}) = \widehat{\mathbf{u}}_{\min}$  (resp.  $L^{3n}(\widehat{\mathbf{v}}_{\min}) = \widehat{\mathbf{v}}_{\min}$ ) is equivalent to  $\xi(\widehat{\mathbf{u}}_{\min}) \in \mathbf{CycStr}(p_0)$  (resp.  $\xi(\widehat{\mathbf{v}}_{\min}) \in \mathbf{CycStr}(p_0)$ ). Then  $q(\mathbf{u}_0) = 1$  (resp.  $q(\mathbf{v}_0) = 1$ ) if and only if  $\mathbf{e}_0 \in \mathfrak{D}$  and  $\mathbf{u}_0 = \rho(\mathbf{e}_0)$  (resp.  $\mathbf{e}_1 \in \mathfrak{D}$  and  $\mathbf{v}_0 = \rho(\mathbf{e}_1)$ ). By Lemma 10,  $\{\mathbf{e}_0, \mathbf{e}_1\} \not\subset \mathbf{CycStr}(p_0)$ . Then  $f_3(\lfloor \mathbf{u}_0 \rfloor_{4n-1}) = f_3(\lfloor \mathbf{v}_0 \rfloor_{4n-1}) = 1$  if and only if one of the following cases holds:

1.  $\mathbf{e}_0 \in \mathbf{CycStr}(p_0)$ ,  $\mathbf{u}_0 = \min S_{4n}(\mathbf{e}_0)$  and  $\{\mathbf{v} \in S_{4n}(\mathbf{e}_0) : f_0(\lfloor \mathbf{v} \rfloor_r) = 1\} \neq \emptyset$ ;
2.  $\mathbf{e}_1 \in \mathbf{CycStr}(p_0)$ ,  $\mathbf{v}_0 = \min S_{4n}(\mathbf{e}_1)$  and  $\{\mathbf{v} \in S_{4n}(\mathbf{e}_1) : f_0(\lfloor \mathbf{v} \rfloor_r) = 1\} \neq \emptyset$ ;
3.  $\mathbf{e}_0 \in \mathfrak{C}_{6n}$ ,  $\mathbf{u}_0 = \min S_{4n}(\mathbf{e}_0)$  and  $\xi(\widehat{\mathbf{u}}_0) = \mathbf{e}_1 \in \mathfrak{C}_{6n}$ ;
4.  $\mathbf{e}_1 \in \mathfrak{C}_{6n}$ ,  $\mathbf{v}_0 = \min S_{4n}(\mathbf{e}_1)$  and  $\xi(\widehat{\mathbf{v}}_0) = \mathbf{e}_0 \in \mathfrak{C}_{6n}$ ;
5.  $\mathbf{e}_0, \mathbf{e}_1 \in \mathfrak{C}_{6n}$ ,  $\mathbf{e}_0 \in \mathfrak{D}$  and  $\mathbf{u}_0 = \rho(\mathbf{e}_0)$ ;
6.  $\mathbf{e}_0, \mathbf{e}_1 \in \mathfrak{C}_{6n}$ ,  $\mathbf{e}_1 \in \mathfrak{D}$  and  $\mathbf{v}_0 = \rho(\mathbf{e}_1)$ .

Considering Statement (i) of Lemma 11, we have

$$f_3(\mathbf{x}) = \begin{cases} 1, & \text{if } \mathbf{x} = \lfloor \mathbf{v} \rfloor_{4n-1}, \text{ where } \mathbf{v} = \rho(\mathbf{c}) \text{ and } \mathbf{c}, \xi(\widehat{\mathbf{v}}) \in \mathfrak{C}_{6n}; & \text{by Cases 3, 4, 5 and 6} \\ 1, & \text{if } \mathbf{x} = \lfloor \mathbf{v} \rfloor_{4n-1}, \text{ where } \mathbf{v} = \rho(\mathbf{c}), \mathbf{c} \in \mathbf{CycStr}(p_0) \\ & \text{and } \{\mathbf{u} \in S_{4n}(\mathbf{c}) : f_0(\lfloor \mathbf{u} \rfloor_r) = 1\} \neq \emptyset; & \text{by Cases 1 and 2} \\ 0, & \text{otherwise.} \end{cases} \quad (3)$$

By Eq.(3) and Lemma 10,  $f_3(\mathbf{x}) = 1$  implies that there exists  $\mathbf{v} \in \{0, 1\}^{4n}$  satisfying  $\mathbf{x} = \lfloor \mathbf{v} \rfloor_{4n-1}$  and  $\lambda(\mathbf{v}) = 1$ .

Hitherto we have shown that Eq.(2) holds, where  $g$  in Eq.(2) is the LFSR  $p_2$ .

By Lemma 3 and Statement (i) of Lemma 11,  $D_{p_2}^f$  is loopless. Assume that  $D_{p_2}^f$  is not acyclic. Then in  $D_{p_2}^f$  there is a walk  $(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{m-1}, \mathbf{c}_m)$  for some  $m \geq 2$ . Specifically,  $\mathbf{c}_i \in \mathbf{CycStr}(p_2)$ ,  $0 \leq i < m$ , are pairwise distinct,  $\mathbf{c}_m = \mathbf{c}_0$ , and for any  $0 \leq i < m$  there is an arc incident from  $\mathbf{c}_i$  to  $\mathbf{c}_{i+1}$ . By Lemma 10 and the definition of  $\lambda$ , any  $\mathbf{c} \in \mathbf{CycStr}(p_0)$  is a source in  $D_{p_2}^f$ . Additionally, for  $\mathbf{c} \in \mathfrak{D}$ , by Statement (i) of Lemma 11 and

$$\{\mathbf{v} \in S_{4n}(\mathbf{c}) : \xi(\widehat{\mathbf{v}}) \in \mathfrak{C}_{6n} \text{ and } \widehat{\mathbf{v}} = \min S_{4n}(\xi(\widehat{\mathbf{v}}))\} = \emptyset,$$

no arc is incident from a cycle in  $\mathfrak{C}_{6n}$  to  $\mathbf{c}$ , i.e., any arc entering  $\mathbf{c}$  leaves from a source in  $\mathbf{CycStr}(p_0)$ . Besides, as shown in the proof of Lemma 11,  $\rho(\xi(\iota^{4n})) = \iota^{4n}$  and  $\xi(\widehat{\iota^{4n}}) = [0]$ , then  $\xi(\iota^{4n})$  is a sink in  $D_{p_2}^f$ . Therefore,  $\xi(\iota^{4n}) \neq \mathbf{c}_i \in \mathfrak{C}_{6n} \setminus \mathfrak{D}$  and  $\rho(\mathbf{c}_i) = \min S_{4n}(\mathbf{c}_i)$ ,  $0 \leq i < m$ . Noticing  $\widehat{\rho(\mathbf{c}_i)} \in S_{4n}(\mathbf{c}_{i+1})$ ,  $0 \leq i < m$ , by Lemma 3, we have  $\min S_{4n}(\mathbf{c}_{i+1}) < \min S_{4n}(\mathbf{c}_i)$  for  $0 \leq i < m$ , implying  $\min S_{4n}(\mathbf{c}_0) < \min S_{4n}(\mathbf{c}_0)$ , which is ridiculous. Therefore, the assumption is absurd and  $D_{p_2}^f$  is acyclic.

Till now we have proved that Eq.(2) holds and  $D_{p_2}^f$  is acyclic, where  $g$  is the LFSR  $p_2$ . By Lemma 7, Statement (i) of this lemma is proved.

Now we prove Statement (ii) of this lemma. Suppose  $\mathbf{c} \in \mathfrak{C}_{6n}$ .

- If  $\xi(\iota^{4n} \oplus \min S_{4n}(\mathbf{c})) \in \mathfrak{C}_{6n}$ , then  $\mathbf{c} \notin \mathfrak{D}$ ,  $\rho(\mathbf{c}) = \min S_{4n}(\mathbf{c})$  and  $\lambda(\rho(\mathbf{c})) = 1$ . By Eq.(3), an arc leaves  $\mathbf{c}$ .
- If  $\xi(\iota^{4n} \oplus \min S_{4n}(\mathbf{c})) \in \mathbf{CycStr}(p_0)$  and

$$\{\mathbf{v} \in S_{4n}(\mathbf{c}) : \xi(\widehat{\mathbf{v}}) \in \mathfrak{C}_{6n} \text{ and } \widehat{\mathbf{v}} = \min S_{4n}(\xi(\widehat{\mathbf{v}}))\} \neq \emptyset.$$

Let  $\mathbf{v}_0 \in S_{4n}(\mathbf{c})$  satisfy  $\xi(\widehat{\mathbf{v}_0}) \in \mathfrak{C}_{6n}$  and  $\widehat{\mathbf{v}_0} = \min S_{4n}(\xi(\widehat{\mathbf{v}_0}))$ . Clearly,  $\xi(\widehat{\mathbf{v}_0}) \notin \mathfrak{D}$ . Then  $\rho(\xi(\widehat{\mathbf{v}_0})) = \min S_{4n}(\xi(\widehat{\mathbf{v}_0})) = \widehat{\mathbf{v}_0}$  and  $\lambda(\widehat{\mathbf{v}_0}) = 1$ . By Eq.(3), an arc enters  $\mathbf{c}$ .

- If  $\xi(\iota^{4n} \oplus \min S_{4n}(\mathbf{c})) \in \mathbf{CycStr}(p_0)$  and

$$\{\mathbf{v} \in S_{4n}(\mathbf{c}) : \xi(\widehat{\mathbf{v}}) \in \mathfrak{C}_{6n} \text{ and } \widehat{\mathbf{v}} = \min S_{4n}(\xi(\widehat{\mathbf{v}}))\} = \emptyset,$$

then  $\mathbf{c} \in \mathfrak{D}$ . By Statement (i) of Lemma 11 and Eq.(3), an arc is incident from  $\mathbf{c}$  to a cycle in  $\mathfrak{C}_{6n} \setminus \mathfrak{D}$ .

Till now Statement (ii) of this lemma is proved.

Now we prove Statement (iii) of this lemma. Since  $\lambda(\mathbf{v}) = 1$  occurs only if  $\xi(\widehat{\mathbf{v}}) \in \mathfrak{C}_{6n}$ , in  $D_{p_2}^f$  no arc enters any  $\mathbf{c} \in \mathbf{CycStr}(p_0)$ . Since  $r \leq 2n$  and  $\bigcup_{\mathbf{c} \in \mathbf{CycStr}(p_0)} S_{2n}(\mathbf{c}) = \{0, 1\}^{2n}$ , we have

$$\left\{ \lfloor \mathbf{v} \rfloor_r : \mathbf{v} \in \bigcup_{\mathbf{c} \in \mathbf{CycStr}(p_0)} S_{4n}(\mathbf{c}) \right\} = \left\{ \lfloor \mathbf{v} \rfloor_r : \mathbf{v} \in \bigcup_{\mathbf{c} \in \mathbf{CycStr}(p_0)} S_{2n}(\mathbf{c}) \right\} = \{0, 1\}^r.$$

By Lemma 10,  $\lambda(\rho(\mathbf{c})) = 1$  for any  $\mathbf{c} \in \mathbf{CycStr}(p_0)$ . Then by Eq.(3), in  $D_{p_2}^f$  there exists an arc incident from some  $\mathbf{c} \in \mathbf{CycStr}(p_0)$  to some  $\mathbf{d} \in \mathfrak{C}_{6n}$  if and only if  $f_0$  is satisfiable. Thus, Statement (iii) of this lemma is proved.  $\square$

**Lemma 13.** *If  $g$  is a subFSR of the FSR  $f$ , then  $g$  is of stage  $2n$ .*

*Proof.* Let  $g$  be of stage  $m$ . By Lemmas 4,  $\sum_{\mathbf{d} \in \mathbf{CycStr}(g)} \text{per}(\mathbf{d}) = 2^m$ . By Lemmas 2, 8 and Statement (i) of 12, for any  $\mathbf{d} \in \mathbf{CycStr}(g)$ ,  $\text{per}(\mathbf{d}) \equiv |\{\mathbf{0}^{4n}\} \cap S_{4n}(\mathbf{d})| \pmod{3n}$ . Then we have an integer equation  $a + 3nb = 2^m$ , where  $a \in \{0, 1\}$  and  $0 \leq b < 2^{4n}/(3n)$ . Since  $2n = \min\{i > 0 : 3n \mid (2^i - 1)\}$ , where  $n = 3^k$  for some  $1 \leq k \in \mathbb{Z}$ , we have  $a = 1$  and  $2n \mid m$ . Hence,  $m = 2n < 4n$ .  $\square$

**Lemma 14.** *The FSR  $f$  is irreducible if and only if the Boolean circuit  $f_0$  is satisfiable.*

*Proof.* Suppose  $f_0$  to be unsatisfiable. By Statements (i) and (iii) of Lemma 12,  $\mathbf{CycStr}(p_0) \subset \mathbf{CycStr}(f)$ . By Lemma 2,  $p_0$  is a subFSR of  $f$  and hence  $f$  is reducible.

Suppose  $f_0$  to be satisfiable. Assume that  $h$  is a subFSR of  $f$ . By Statement (i) of Lemma 12,

$$\mathbf{CycStr}(h) \subset \mathbf{CycStr}(p_2). \quad (4)$$

Furthermore, by Statements (i) and (ii) of Lemma 12, any cycle in  $\mathfrak{C}_{6n}$  joins with other cycles to combine a cycle in  $\mathbf{CycStr}(f)$ , implying

$$(\mathbf{CycStr}(p_2) \setminus \mathbf{CycStr}(p_0)) \cap \mathbf{CycStr}(f) = \emptyset. \quad (5)$$

Similarly, by Statements (i) and (iii) of Lemma 12, if  $f_0$  is satisfiable, then

$$\mathbf{CycStr}(p_0) \not\subset \mathbf{CycStr}(f). \quad (6)$$

By Eqs.(4), (5), (6) and Lemma 2, we get

$$\mathbf{CycStr}(h) \subset \mathbf{CycStr}(f) \cap \mathbf{CycStr}(p_2) \subset \mathbf{CycStr}(f) \cap \mathbf{CycStr}(p_0) \subsetneq \mathbf{CycStr}(p_0).$$

By Lemma 13,  $h$  is of stage  $2n$ . However, by Lemma 4,

$$2^{2n} = \sum_{\mathbf{c} \in \mathbf{CycStr}(h)} \text{per}(\mathbf{c}) < \sum_{\mathbf{c} \in \mathbf{CycStr}(p_0)} \text{per}(\mathbf{c}) = 2^{2n},$$

which is absurd. Therefore,  $f$  is irreducible. □

**PROBLEM: FSR IRREDUCIBILITY**

INSTANCE: An FSR  $f$  with its feedback logic  $f_1$  as a Boolean circuit of size **SIZE**( $f_1$ ).

QUESTION: Is  $f$  irreducible?

By Lemmas 1, 9 and 14, Algorithm 1 is a polynomial-time Karp reduction from CIRCUIT SATISFIABILITY to FSR IRREDUCIBILITY. Therefore, we conclude that

**Theorem 1.** *The FSR IRREDUCIBILITY problem is NP-hard.*

## 4 NP-hardness of deciding indecomposable FSRs

**Lemma 15.** *Let  $f_0$  be an  $r$ -input Boolean logic and*

$$f_2(\mathbf{x}) = \begin{cases} 0, & \text{if } \mathbf{x} = \mathbf{0}^r; \\ 1, & \text{if } \mathbf{x} = \mathbf{1}^r \text{ and } f_0(\mathbf{1}^r) = 1; \\ f_0(\mathbf{0}^r), & \text{if } \mathbf{x} = \mathbf{1}^r \text{ and } f_0(\mathbf{1}^r) = 0; \\ f_0(\mathbf{x}), & \text{otherwise.} \end{cases} \quad (7)$$

*Then the Boolean function  $f_2$  is satisfiable if and only if  $f_0$  is satisfiable.*

Below Algorithm 2 transforms a given Boolean circuit to an FSR.

Figure 8 is a sketch of  $f_2$ . Following Algorithm 2, we describe  $f_3$  with Figure 9.

In the rest of this section, we use notations  $f_0$ ,  $f_2$ ,  $f_3$  and  $f$  defined in Algorithm 2.

Clearly,  $f$  is a nonsingular FSR.

Similar to Lemma 9, we count gates in Figure 9 and derive the lemma below.

**Output:** A  $(2n+1)$ -stage FSR  $f$ , where  $k = \min \{i \in \mathbb{Z} : i \geq \log_3(r/2)\}$  and  $n = 3^k$ .

- 1: Construct an  $r$ -input Boolean circuit  $f_2$  defined by Eq.(7).
- 2: {Construct a  $2n$ -input Boolean circuit  $f_3$  with its pseudocode in Lines 3-13. In the rest of this section,  $L$  denotes the state transformation of the LFSR  $x^{2n} \oplus x^n \oplus 1$ . }
- 3: Let  $(x_1, x_2, \dots, x_{2n})$  be the input of  $f_3$ .
- 4:  $\mathbf{u}_0 = (x_{2n} \oplus x_n \oplus x_1, x_1 \oplus x_2, x_2 \oplus x_3, \dots, x_{2n-1} \oplus x_{2n})$ .
- 5: **for**  $i = 1$  to  $3n$  **do**
- 6:      $\mathbf{u}_i = L(\mathbf{u}_{i-1})$ .
- 7:      $a_i = f_2(\lfloor \mathbf{u}_i \rfloor_r)$ .
- 8: **end for**
- 9: **if**  $\mathbf{u}_{3n} = \min \{ \mathbf{u}_i : 1 \leq i \leq 3n \}$  and  $a_1 \vee a_2 \vee \dots \vee a_{3n} = 1$  **then**
- 10:     The Boolean circuit  $f_3$  returns 1.
- 11: **else**
- 12:     The Boolean circuit  $f_3$  returns 0.
- 13: **end if**
- 14: **return** the FSR  $f(x_0, \dots, x_{2n+1}) = x_{2n+1} \oplus x_{2n} \oplus x_{n+1} \oplus x_n \oplus x_1 \oplus x_0 \oplus f_3(x_1, x_2, \dots, x_{2n})$ .

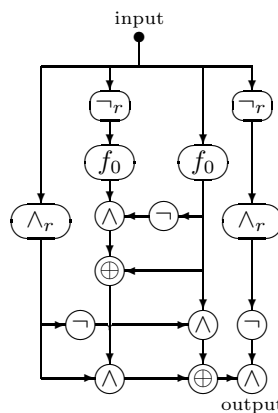


Figure 8: A diagram of the Boolean circuit  $f_2$





If  $\mathbf{v} \in \bigcup_{\mathbf{c} \in \mathbf{CycStr}(p_0)} S_{2n+1}(\mathbf{c})$ . clearly,  $\chi(\mathbf{v}) = v_0 \oplus v_n \oplus v_{2n} = 0$ . Suppose  $\mathbf{v} \in \bigcup_{\mathbf{c} \in \overline{\mathbf{CycStr}(p_0)}} S_{2n+1}(\mathbf{c})$ . By Lemma 8,  $\bar{\mathbf{v}} \in \bigcup_{\mathbf{c} \in \mathbf{CycStr}(p_0)} S_{2n+1}(\mathbf{c})$ . Then by Statement (i),  $\chi(\mathbf{v}) = 1 \oplus \chi(\bar{\mathbf{v}}) = 1$ . Statement (iii) is proved.

By Lemma 8,

$$\left( \bigcup_{\mathbf{c} \in \mathbf{CycStr}(p_0)} S_{2n+1}(\mathbf{c}) \right) \cup \left( \bigcup_{\mathbf{c} \in \overline{\mathbf{CycStr}(p_0)}} S_{2n+1}(\mathbf{c}) \right) = \{0, 1\}^{2n+1}.$$

Then Statement (iv) follows from Statement (i) and (iii).

Additionally, Statement (v) holds because

$$\begin{aligned} \lfloor L_1(\mathbf{v}) \rfloor_{2n} &= (v_2, \dots, v_{2n}, v_{2n} \oplus v_{n+1} \oplus v_n \oplus v_1 \oplus v_0) \\ &= (v_2, \dots, v_{2n}, v_{n+1} \oplus v_1 \oplus \chi(\mathbf{v})) \\ &= L((v_1, v_2, \dots, v_{2n})) \oplus \mathbf{w}_0 \\ &= L(\lfloor \mathbf{v} \rfloor_{2n}) \oplus \mathbf{w}_0. \end{aligned}$$

□

**Lemma 18.** Let the map  $\lambda : \{0, 1\}^{2n+1} \rightarrow \{0, 1\}$  be defined as

$$\lambda(\mathbf{v}) = \begin{cases} 1, & \text{if } \chi(\mathbf{v}) = 0 \text{ and } \pi(\mathbf{v}) = \min \{L^i(\pi(\mathbf{v})) : 1 \leq i \leq 3n\}; \\ 0, & \text{otherwise.} \end{cases}$$

Let  $D_{p_1}^f$  be the graph defined as in Lemma 7 (Recall that  $f$  and  $f_3$  are given in Algorithm 2). Then the following statements hold: (i) Statements (i) and (ii) of Lemma 7 hold, where  $g$  in Lemma 7 is the LFSR  $p_1$ . (ii) If  $f_2$  is satisfiable, then  $\mathbf{CycStr}(p_0) \not\subset \mathbf{CycStr}(f)$  and there exists  $\mathbf{v} \in \{0, 1\}^{2n+1}$  satisfying  $f_3(\lfloor \mathbf{v} \rfloor_{2n}) = 1$  and  $\chi(\mathbf{v}) = 0$ .

*Proof.* Suppose  $\mathbf{v} \in S_{2n+1}(\mathbf{c})$ , where  $\mathbf{c} \in \mathbf{CycStr}(p_1)$ . By Statement (i) of Lemma 17, Lemmas 6 and 8, we get

$$\{L^i(\pi(\mathbf{v})) : 1 \leq i \leq 3n\} = \{\pi(L_1^i(\mathbf{v})) : 1 \leq i \leq 3n\} = \{\pi(\mathbf{u}) : \mathbf{u} \in S_{2n+1}(\mathbf{c})\}. \quad (8)$$

Besides, by Statements (ii) of Lemma 17, there exists a unique vector  $\mathbf{u}$  in  $S_{2n+1}(\mathbf{c})$  satisfying  $\pi(\mathbf{u}) = \min \{\pi(\mathbf{u}) : \mathbf{u} \in S_{2n+1}(\mathbf{c})\}$ . Thus, by Statement (iii) of Lemma 17, we have

$$|\{\mathbf{v} \in S_{2n+1}(\mathbf{c}) : \lambda(\mathbf{v}) = 1\}| = \begin{cases} 1, & \text{if } \mathbf{c} \in \mathbf{CycStr}(p_0); \\ 0, & \text{if } \mathbf{c} \in \overline{\mathbf{CycStr}(p_0)}. \end{cases} \quad (9)$$

By Statement (i) of Lemma 17,  $\lambda(\mathbf{v}) \cdot \lambda(\hat{\mathbf{v}}) = 0$  for any  $\mathbf{v} \in \{0, 1\}^{2n+1}$ .

In Algorithm 2,  $\mathbf{x} = (x_1, x_2, \dots, x_{2n})$  and  $\mathbf{u}_0 = \pi(\mathbf{y})$ , where  $\mathbf{y} = (x_{2n} \oplus x_n, x_1, x_2, \dots, x_{2n})$  is the unique vector in  $\{0, 1\}^{2n+1}$  satisfying  $\chi(\mathbf{y}) = 0$  and  $\lfloor \mathbf{y} \rfloor_{2n} = \mathbf{x}$ . Let  $\mathbf{c}$  be the cycle satisfying  $\mathbf{y} \in S_{2n+1}(\mathbf{c})$ . By Lemmas 6, 8 and Eq.(8),  $\mathbf{u}_{3n} = \min \{L^i(\mathbf{u}_0) : 1 \leq i \leq 3n\}$  is equivalent to  $\mathbf{u}_0 = \min \{\pi(\mathbf{v}) : \mathbf{v} \in S_{2n+1}(\mathbf{c})\}$ . By Eq.(8),

$$\{1 \leq i \leq 3n : f_2(\lfloor L^i(\mathbf{u}_0) \rfloor_r) = 1\} \neq \emptyset$$

is equivalent to

$$\{\mathbf{u} \in S_{2n+1}(\mathbf{c}) : f_2(\lfloor \pi(\mathbf{u}) \rfloor_r) = 1\} \neq \emptyset.$$

Thus, by Algorithm 2, we have the following claim.

*Claim.*  $f_3(\mathbf{x}) = 1$  if and only if  $\lambda(\mathbf{y}) = 1$  and  $\{\mathbf{v} \in S_{2n+1}(\mathbf{c}) : f_2(\lfloor \pi(\mathbf{v}) \rfloor_r) = 1\} \neq \emptyset$ .

If  $f_3(\mathbf{x}) = 1$ , then  $\lambda(\mathbf{y}) = 1$  and  $\lfloor \mathbf{y} \rfloor_{2n} = \mathbf{x}$ . Therefore, Eq.(2) holds, where  $g$  in Lemma 7 is the LFSR  $p_1$ .

Furthermore, by Statement (iv) of Lemma 17 and Eq.(9), any arc of  $D_{p_1}^f$  is incident from a cycle in  $\mathbf{CycStr}(p_0)$  to a cycle in  $\overline{\mathbf{CycStr}(p_0)}$ . Hence,  $D_{p_1}^f$  is acyclic.

Till now we have proved that Eq.(2) holds and  $D_{p_1}^f$  is acyclic, where  $g$  in Eq.(2) is the LFSR  $p_1$ . By Lemma 7, Statements (i) and (ii) of Lemma 7 hold and Statement (i) of this lemma is proved, where  $g$  in Lemma 7 is the LFSR  $p_1$ .

Now we prove Statement (ii) of this lemma. Suppose that  $f_2$  is satisfiable. Since  $D_{p_1}^f$  is acyclic, by Statement (i) of Lemma 7, it is sufficient to prove that not every  $\mathbf{c} \in \mathbf{CycStr}(p_0)$  is isolated in  $D_{p_1}^f$ .

Following from Eq.(9) and the claim above, for  $\mathbf{c} \in \mathbf{CycStr}(p_0)$ , there exists  $\mathbf{v} \in S_{2n+1}(\mathbf{c})$  satisfying  $\lambda(\mathbf{v}) = 1$  and  $f_3(\lfloor \mathbf{v} \rfloor_{2n}) = 1$  if and only if  $\{\mathbf{v} \in S_{2n+1}(\mathbf{c}) : f_2(\lfloor \pi(\mathbf{v}) \rfloor_r) = 1\} \neq \emptyset$ .

By Lemma 8 and Statement (ii) of Lemma 17, the map  $\pi$  gives a bijection from  $\bigcup_{\mathbf{c} \in \mathbf{CycStr}(p_0)} S_{2n+1}(\mathbf{c})$  to  $\{0, 1\}^{2n}$ . Thus, seeing  $r \leq 2n$ , we get

$$\left\{ \lfloor \pi(\mathbf{v}) \rfloor_r : \mathbf{v} \in \bigcup_{\mathbf{c} \in \mathbf{CycStr}(p_0)} S_{2n+1}(\mathbf{c}) \right\} = \{ \lfloor \mathbf{v} \rfloor_r : \mathbf{v} \in \{0, 1\}^{2n} \} = \{0, 1\}^r.$$

Therefore, on one hand, there exists  $\mathbf{v} \in \{0, 1\}^{2n+1}$  satisfying  $f_3(\lfloor \mathbf{v} \rfloor_{2n}) = 1$  and  $\chi(\mathbf{v}) = 0$ ; On the other hand, in  $D_{p_1}^f$  there exists at least one arc incident from a cycle in  $\mathbf{CycStr}(p_0)$ , i.e., some  $\mathbf{c} \in \mathbf{CycStr}(p_0)$  is not isolated in  $D_{p_1}^f$ . By Statement (i) of this lemma,  $\mathbf{c}$  joins with other cycles in  $\mathbf{CycStr}(p_1)$  to combine one cycle in  $\mathbf{CycStr}(f)$ , and hence  $\mathbf{c} \notin \mathbf{CycStr}(f)$ , yielding  $\mathbf{CycStr}(p_0) \not\subset \mathbf{CycStr}(f)$ .  $\square$

**Lemma 19.** *If  $f_2$  is satisfiable and  $g$  is a subFSR of  $f$  satisfying  $[0] \in \mathbf{CycStr}(g)$ , then  $g$  is the LFSR  $x_1 \oplus x_0$ , i.e.,  $\mathbf{CycStr}(g) = \{[0], [1]\}$ .*

*Proof.* Let  $g$  be an  $m$ -stage subFSR of  $f$ .

By Lemma 4, we have  $2^m = \sum_{\mathbf{d} \in \mathbf{CycStr}(g)} \text{per}(\mathbf{d})$ . Furthermore, by Lemma 8 and Statement (i) of 18, we have

$$\text{per}(\mathbf{d}) \equiv |\{0^{2n+1}, 1^{2n+1}\} \cap S_{2n+1}(\mathbf{d})| \pmod{3n}.$$

Since for any  $\mathbf{v} \in \{0, 1\}^{2n+1}$ , there exists a unique cycle  $\mathbf{c} \in \mathbf{CycStr}(f)$  satisfying  $\mathbf{v} \in S_{2n+1}(\mathbf{c})$ , we get an integer equation

$$3na + b = 2^m, \quad (10)$$

where  $1 \leq m \leq 2n$ ,  $0 \leq a \leq 2(2^{2n} - 1)/(3n)$  and  $b \in \{0, 1, 2\}$ . Since  $2n = \min \{0 < i \in \mathbb{Z} : 3n \mid (2^i - 1)\}$ , where  $n = 3^k$  for some  $1 \leq k \in \mathbb{Z}$ , Eq.(10) holds only if (i)  $b = 1$  and  $m = 2n$  or (ii)  $b = 2$  and  $m = 1$ . So, we only have to consider two possible cases below.

Case (i):  $g$  is of stage  $2n$ . By Statement (i) of Lemma 18,  $\mathbf{CycStr}(g) \subset \mathbf{CycStr}(p_1)$ . Denote

$$\begin{aligned} V_0 &= \{\mathbf{v} \in \{0, 1\}^{2n} : \mathbf{v} \in S_{2n}(\mathbf{c}), \mathbf{c} \in \mathbf{CycStr}(g) \cap \mathbf{CycStr}(p_0)\}; \\ V_1 &= \{\mathbf{v} \in \{0, 1\}^{2n} : \mathbf{v} \in S_{2n}(\mathbf{c}), \mathbf{c} \in \mathbf{CycStr}(g) \cap \overline{\mathbf{CycStr}(p_0)}\}. \end{aligned}$$

Since  $b = 1$  in Eq.(10), by Lemma 8,  $\mathbf{CycStr}(g)$  consists of  $[0]$  and  $(2^{2n} - 1)/(3n)$   $3n$ -cycles. Moreover, by Statement (ii) of Lemma 18, we have

$$|\mathbf{CycStr}(g) \cap \overline{\mathbf{CycStr}(p_0)}| \geq 1,$$

implying  $V_1 \neq \emptyset$ . Besides, as the states of the  $2n$ -stage FSR  $g$ ,  $V_0 \cup V_1 = \{0, 1\}^{2n}$  and  $V_0 \cap V_1 = \emptyset$ . For  $V \subset \{0, 1\}^{2n}$ , denote  $L(V) = \{L(\mathbf{v}) : \mathbf{v} \in V\}$ . On one hand, by Lemma 6,  $L(V_0) = V_0$ . Because  $L$  is bijective on  $\{0, 1\}^{2n}$ , we have  $L(V_1) = V_1$ . Denote  $\mathbf{w}_0 = (0, \dots, 0, 1) \in \{0, 1\}^{2n}$ . On the other hand, by Statements (iii) and (v) of Lemma 17, we have  $L(\mathbf{v}) \oplus \mathbf{w}_0 \in V_1$  for any  $\mathbf{v} \in V_1$ . Thus, both  $\mathbf{v} \mapsto L(\mathbf{v})$  and

$\mathbf{v} \mapsto L(\mathbf{v}) \oplus \mathbf{w}_0$  are closed on  $V_1$ . Since the linear transformation  $L$  has its irreducible minimal polynomial  $p_0$  of degree  $2n$ ,  $L^i(\mathbf{w}_0)$ ,  $i = 0, \dots, 2n-1$ , is a basis of the linear space  $\{0, 1\}^{2n}$ . Then for any  $\mathbf{v}_0 \in V_1$ , there exist  $b_i \in \{0, 1\}$ ,  $1 \leq i \leq 3n$ , satisfying  $\mathbf{v}_0 = \bigoplus_{i=1}^{3n} b_i \cdot L^{3n-i}(\mathbf{w}_0)$ . Let  $\mathbf{v}_i = L(\mathbf{v}_{i-1}) \oplus (b_i \cdot \mathbf{w}_0)$ ,  $1 \leq i \leq 3n$ . Then  $\mathbf{v}_i \in V_1$ ,  $1 \leq i \leq 3n$ . However, by Lemmas 6 and 8,  $L^{3n}$  is an identity map. Hence,  $\mathbf{v}_{3n} = L^{3n}(\mathbf{v}_0) \oplus \left(\bigoplus_{i=1}^{3n} b_i \cdot L^{3n-i}(\mathbf{w}_0)\right) = \mathbf{0}^{2n} \in V_0$ , yielding  $\mathbf{0}^{2n} \in V_0 \cap V_1 = \emptyset$ , which is ridiculous. Therefore, Case (i) does not occur.

Case(ii).  $g$  is of stage 1. Since  $[0] \in \mathbf{CycStr}(g)$ , we have  $\mathbf{CycStr}(g) = \{[0], [1]\}$ , i.e.,  $g$  is the LFSR  $x_1 \oplus x_0$ .  $\square$

**Lemma 20.** *If  $f_2$  is satisfiable, then for any FSR  $h$ ,  $f \neq h * (x_1 \oplus x_0)$ .*

*Proof.* Assume  $f = h * (x_1 \oplus x_0)$ . Then  $h$  is a  $2n$ -stage FSR and  $h(x_0, x_1, \dots, x_{2n}) = x_{2n} \oplus h_1(x_0, x_1, \dots, x_{2n-1})$ , where  $h_1$  is a  $2n$ -input Boolean logic. By Statement (ii) of Lemma 18, if  $f_2$  is satisfiable, then there exists  $\mathbf{v}_0 \in \{0, 1\}^{2n+1}$  satisfying  $f_3(\lfloor \mathbf{v}_0 \rfloor_{2n}) = 1$  and  $\chi(\mathbf{v}_0) = 0$ . Let  $f_1$  denote the feedback logic of  $f$  and  $\mathbf{v}_0 = (a_0, a_1, \dots, a_{2n})$ . Then  $f_1(\mathbf{v}_0) = a_1 \oplus a_{n+1} \oplus \chi(\mathbf{v}_0) \oplus f_3(\lfloor \mathbf{v}_0 \rfloor_{2n}) = a_1 \oplus a_{n+1} \oplus 1$ . Thus,  $f(\mathbf{v}_0 \parallel f_1(\mathbf{v}_0)) = h(\pi(\mathbf{v}_0) \parallel (a_{2n} \oplus a_1 \oplus a_{n+1} \oplus 1)) = 0$ , yielding

$$h_1(\pi(\mathbf{v}_0)) = a_{2n} \oplus a_1 \oplus a_{n+1} \oplus 1. \quad (11)$$

Let  $\mathbf{u}_0 = \widehat{\mathbf{v}_0}$ . By Statements (i) and (ii) of Lemma 17,  $\chi(\mathbf{u}_0) = 0$  and  $\pi(\mathbf{u}_0) = \widehat{\pi(\mathbf{v}_0)}$ . If

$$\pi(\mathbf{u}_0) \neq \min \{L^i(\pi(\mathbf{u}_0)) : 1 \leq i \leq 3n\},$$

then  $f_3(\lfloor \overline{\mathbf{v}_0} \rfloor_{2n}) = f_3(\lfloor \mathbf{u}_0 \rfloor_{2n}) = 0$ . Otherwise, assume  $\pi(\mathbf{u}_0) = \min \{L^i(\pi(\mathbf{u}_0)) : 1 \leq i \leq 3n\}$ . Since  $f_3(\lfloor \mathbf{v}_0 \rfloor_{2n}) = 1$ , we get

$$\pi(\mathbf{v}_0) = \min \{L^i(\pi(\mathbf{v}_0)) : 1 \leq i \leq 3n\}.$$

As  $\pi(\mathbf{u}_0) = \widehat{\pi(\mathbf{v}_0)}$ , by Lemmas 3 and 8, we have  $\{\pi(\mathbf{v}_0), \pi(\mathbf{u}_0)\} = \{\mathbf{0}^{2n}, \mathbf{t}^{2n}\}$ . Considering  $\chi(\mathbf{v}_0) = \chi(\mathbf{u}_0) = 0$ , we have

$$\{\mathbf{v}_0, \mathbf{u}_0\} = \{\mathbf{0}^{2n+1}, \overline{\mathbf{t}^{2n+1}}\}.$$

Because  $f_3(\lfloor \mathbf{v}_0 \rfloor_{2n}) = 1$  while  $f_3(\mathbf{0}^{2n}) = 0$ , we have  $\mathbf{u}_0 = \mathbf{0}^{2n+1}$ , yielding  $f_3(\lfloor \overline{\mathbf{v}_0} \rfloor_{2n}) = f_3(\lfloor \mathbf{u}_0 \rfloor_{2n}) = 0$ .

We have proved  $f_3(\lfloor \overline{\mathbf{v}_0} \rfloor_{2n}) = 0$ . Then  $F(\overline{\mathbf{v}_0}) = L_1(\overline{\mathbf{v}_0})$ , where  $F$  is the state transformation of  $f$ . Using  $\chi(\mathbf{v}_0) = 0$  and Statements (i)-(ii) of Lemma 17, we get

$$f(\overline{\mathbf{v}_0} \parallel (a_1 \oplus a_{n+1} \oplus \chi(\overline{\mathbf{v}_0}) \oplus f_3(\lfloor \overline{\mathbf{v}_0} \rfloor_{2n}))) = h(\pi(\mathbf{v}_0) \parallel (a_{2n} \oplus a_1 \oplus a_{n+1})) = 0,$$

implying

$$h_1(\pi(\mathbf{v}_0)) = a_{2n} \oplus a_1 \oplus a_{n+1}. \quad (12)$$

Our assumption  $f = h * (x_1 \oplus x_0)$  leads to contradictory Eqs. (11) and (12). The proof is completed.  $\square$

**Lemma 21.** *[4] Let  $h$  be an  $m$ -stage decomposable FSR satisfying  $h(\mathbf{0}^{m+1}) = 0$ . Then there exist two FSRs  $h_1$  and  $h_2$  such that  $h = h_1 * h_2$ , where  $h_2$  is a  $k$ -stage FSR for some  $1 \leq k < m$  and  $[0] \in \mathbf{CycStr}(h_2)$ . Particularly,  $h_2$  is a subFSR of  $h$  and  $h$  is reducible.*

*Proof.* Since  $h$  is decomposable, we assume  $h = h'_1 * h'_2$ , where  $h'_2$  is a  $k$ -stage FSR,  $1 \leq k < m$ . If  $h'_2(\mathbf{0}^{k+1}) = 0$ , let  $h_1 = h'_1$  and  $h_2 = h'_2$ . Assume  $h'_2(\mathbf{0}^{k+1}) = 1$ . Let  $h_2 = h'_2 \oplus 1$  and  $h_1(x_0, x_1, \dots, x_{m-k}) = h'_1(x_0 \oplus 1, x_1 \oplus 1, \dots, x_{m-k} \oplus 1)$ . Then  $h = h'_1 * h'_2 = h_1 * h_2$  and  $h_2(\mathbf{0}^{k+1}) = h'_2(\mathbf{0}^{k+1}) \oplus 1 = 0$ . Besides,  $h_2(\mathbf{0}^{k+1}) = 0$  is equivalent to  $[0] \in \mathbf{CycStr}(h_2)$ .

Because  $h_1(\mathbf{0}^{m-k+1}) = h_1(h_2(\mathbf{0}^{k+1}), h_2(\mathbf{0}^{k+1}), \dots, h_2(\mathbf{0}^{k+1})) = h(\mathbf{0}^{m+1}) = 0$ , we have  $G(h_2) \subset G(h_1; h_2) = G(h)$ , where  $G(h_1; h_2)$  is the set of sequences generated by the cascade connection of  $h_1$  into  $h_2$ . Therefore,  $h_2$  is a subFSR of  $h$  and  $h$  is reducible.  $\square$

The idea of Lemma 21 was given by [4] and here we reinterpret it for readability.

**Lemma 22.** *The FSR  $f$  is indecomposable if and only if the Boolean circuit  $f_0$  is satisfiable.*

*Proof.* Consider two cases below.

Case (i):  $f_0$  is satisfiable. By Lemma 15,  $f_2$  is satisfiable. Assume  $f$  to be decomposable. Since  $f_2(\mathbf{0}^r) = 0$ , by Algorithm 2, we have  $f_3(\mathbf{0}^{2n}) = 0$  and  $f(\mathbf{0}^{2n+1}) = 0$ , implying  $[0] \in \mathbf{CycStr}(f)$ . By Lemma 21, there exist FSRs  $h$  and  $g$  such that  $f = h * g$ , where  $g$  is a subFSR of  $f$  satisfying  $[0] \in \mathbf{CycStr}(g)$ . By Lemma 19,  $g$  is the LFSR  $x_1 \oplus x_0$ . However, by Lemma 20,  $f \neq h * (x_1 \oplus x_0)$ . Hence, the assumption is absurd and  $f$  is indecomposable.

Case (ii):  $f_0$  is unsatisfiable. By Lemma 15,  $f_2$  is unsatisfiable. By Algorithm 2,  $f_3(\mathbf{x}) = 0$  for any  $\mathbf{x} \in \{0, 1\}^{2n}$ . Then  $f$  is exactly the LFSR  $p_1$  and  $f(x_0, x_1, \dots, x_{2n}) = (x_{2n} \oplus x_n \oplus x_0) * (x_1 \oplus x_0)$ . So,  $f$  is decomposable.  $\square$

**PROBLEM:** FSR INDECOMPOSABILITY

INSTANCE: An FSR  $f$  with its feedback logic  $f_1$  as a Boolean circuit of size **SIZE**( $f_1$ ).

QUESTION: Is  $f$  indecomposable?

By Lemmas 1, 16 and 22, Algorithm 2 is a polynomial-time Karp reduction from CIRCUIT SATISFIABILITY to FSR INDECOMPOSABILITY. Therefore, we conclude that

**Theorem 2.** *The FSR INDECOMPOSABILITY problem is **NP**-hard.*

## 5 Conclusion

Deciding irreducibility/indecomposability of FSRs is meaningful for sophisticated circuit implementation and security analysis of stream ciphers. Here we have proved both the decision problems are **NP**-hard. Assuming  $\mathbf{P} \neq \mathbf{NP}$ , where  $\mathbf{P}$  is the class of decision problems computed by polynomial-time deterministic Turing machines, it is intractable to find a polynomial-time computable algorithm for either problem.

Furthermore, it is still of theoretical interests to determine the computational complexity of search versions of FSR reducibility/decomposability, i.e., to find a subFSR/factor of a given FSR, where  $g$  and  $h$  are called factors of  $f$  if  $f = h * g$ . Besides, provided that the input Boolean circuit is satisfiable, Algorithm 1 (resp. Algorithm 2) constructs an irreducible (resp. indecomposable) FSR. Since it is easy to efficiently find satisfiable Boolean circuits, it remains a question whether Algorithm 1 (resp. Algorithm 2) can be modified to construct a family of irreducible (resp. indecomposable) FSRs with desirable properties in practice.

## 6 Appendices

### 6.1 Appendix: the proof of Statement (i) of Lemma 7

*Proof.* Let  $F$  denote the state transformation of the FSR  $f$ .

By Lemma 6, it is sufficient to prove the following claim.

*Claim:* For any  $\mathbf{u}, \mathbf{v} \in \{0, 1\}^m$ , there exists  $i \geq 0$  satisfying  $F^i(\mathbf{u}) = \mathbf{v}$  if and only if  $\mathbf{u}, \mathbf{v} \in \bigcup_{\mathbf{c} \in \mathfrak{C}} S_m(\mathbf{c})$ , where  $\mathfrak{C}$  is a weakly connected component of  $D_g^f$ .

We prove this claim by induction on the number of arcs in  $D_g^f$ .

If  $D_g^f$  has no arc, then by Eq.(2),  $f_3(\lfloor \mathbf{v} \rfloor_{m-1}) = 0$  for any  $\mathbf{v} \in \{0, 1\}^m$ . Thus,  $\mathbf{CycStr}(g) = \mathbf{CycStr}(f)$  and the claim holds.

Now suppose that  $D_g^f$  has at least one arc.

Because  $D_g^f$  is acyclic, there exists a source  $\mathbf{c}_0 \in \mathbf{CycStr}(g)$  with positive outdegree. Denote  $V = \{\mathbf{v} \in S_m(\mathbf{c}_0) : f_3(\lfloor \mathbf{v} \rfloor_{m-1}) = 1, \lambda(\mathbf{v}) = 1\}$ . By Eq.(2),  $|V| = 1$  and there is a unique arc leaving  $\mathbf{c}_0$ . Denote  $V = \{\mathbf{v}_0\}$ . Let  $\mathbf{c}_1$  denote the unique successor of  $\mathbf{c}_0$ , and let  $\mathfrak{C}$  denote the weakly connected component containing  $\mathbf{c}_0$ . We have  $\mathbf{c}_1 \neq \mathbf{c}_0$  because  $D_g^f$  is acyclic.

Let  $\mathbf{v}_0 = (v_0, v_1, \dots, v_{m-1})$  and

$$\begin{aligned} f'_3(x_1, \dots, x_m) &= f_3(x_1, \dots, x_m) \oplus \prod_{i=1}^{m-1} (x_i \oplus v_i \oplus 1); \\ f'(x_0, x_1, \dots, x_m) &= g(x_0, x_1, \dots, x_m) \oplus f'_3(x_1, \dots, x_m). \end{aligned}$$

Define a directed graph  $D_g^{f'}$  with the set of vertices  $\mathbf{CycStr}(g)$  such that an arc is incident from  $\mathbf{a}$  to  $\mathbf{b}$  if and only if

$$\{\mathbf{v} \in S_m(\mathbf{a}) : f'_3(\lfloor \mathbf{v} \rfloor_{m-1}) = 1, \lambda(\mathbf{v}) = 1, \widehat{\mathbf{v}} \in S_m(\mathbf{b})\} \neq \emptyset.$$

See that  $f'_3$  differs from  $f_3$  only at  $(v_1, \dots, v_{m-1})$  with  $f'_3(v_1, \dots, v_{m-1}) = 0$ . Then  $D_g^{f'}$  is obtained by removing the arc leaving  $\mathbf{c}_0$  in  $D_g^f$ . Besides, Eq.(2) also holds for  $f'_3$ .

Denote  $F'$  as the state transformation of  $f'$ . The cycle joining method gives

$$F'(\mathbf{v}) = \begin{cases} F(\widehat{\mathbf{v}}), & \text{if } \mathbf{v} \in \{\mathbf{v}_0, \widehat{\mathbf{v}}_0\}; \\ F(\mathbf{v}), & \text{otherwise.} \end{cases} \quad (13)$$

By induction, the claim above is assumed to hold for  $f'$ . We only have to consider states in  $\bigcup_{\mathbf{c} \in \mathfrak{C}} S_m(\mathbf{c})$ . In  $D_g^{f'}$ ,  $\mathfrak{C} \setminus \{\mathbf{c}_0\}$  and  $\{\mathbf{c}_0\}$  are weakly connected components. Denoting  $p = \text{per}(\mathbf{c}_0)$  and  $q = \sum_{\mathbf{c}_0 \neq \mathbf{c} \in \mathfrak{C}} \text{per}(\mathbf{c})$ , and using Lemma 6, we have

$$\begin{cases} \{F'^i(F(\mathbf{v}_0)) : 0 \leq i < q\} = \bigcup_{\mathbf{c}_0 \neq \mathbf{c} \in \mathfrak{C}} S_m(\mathbf{c}); \\ \{F'^i(F(\widehat{\mathbf{v}}_0)) : 0 \leq i < p\} = S_m(\mathbf{c}_0); \\ F'^{q-1}(F(\mathbf{v}_0)) = \widehat{\mathbf{v}}_0; \\ F'^{p-1}(F(\widehat{\mathbf{v}}_0)) = \mathbf{v}_0. \end{cases} \quad (14)$$

By Eqs. (13) and (14),  $F^{p+q}(\mathbf{v}_0) = \mathbf{v}_0$  and

$$\{F^i(\mathbf{v}_0) : 0 \leq i < p+q\} = \bigcup_{\mathbf{c} \in \mathfrak{C}} S_m(\mathbf{c}).$$

Thus, the claim also holds for  $f$ .

The proof of this claim is complete by induction. □

## 6.2 Appendix: The operation min

The operation “min” outputs the minimum of two integers.

Let  $\min_m$  denote the operation computing the minimum of two  $m$ -bit nonnegative integers. Recall that a vector  $\mathbf{v} = (v_0, v_1, \dots, v_{m-1})$  is identified as the integer  $\sum_{i=0}^{m-1} v_i 2^i$ . For  $m = 1$ , we have  $\min_1(x_0, y_0) = x_0 \wedge y_0$ . For  $m \geq 2$ ,  $\mathbf{x} = (x_0, x_1, \dots, x_{m-1})$  and  $\mathbf{y} = (y_0, y_1, \dots, y_{m-1})$ , we have

$$\begin{aligned} \min_m(\mathbf{x}, \mathbf{y}) &= (x_{m-1} \oplus y_{m-1} \oplus 1) \times (\min_{m-1}(\lceil \mathbf{x} \rceil_{m-1}, \lceil \mathbf{y} \rceil_{m-1}) \parallel x_{m-1}) \\ &\quad \oplus (((x_{m-1} \oplus y_{m-1}) \wedge (x_{m-1} \oplus 1)) \times \mathbf{x}) \\ &\quad \oplus (((x_{m-1} \oplus y_{m-1}) \wedge (y_{m-1} \oplus 1)) \times \mathbf{y}), \end{aligned}$$

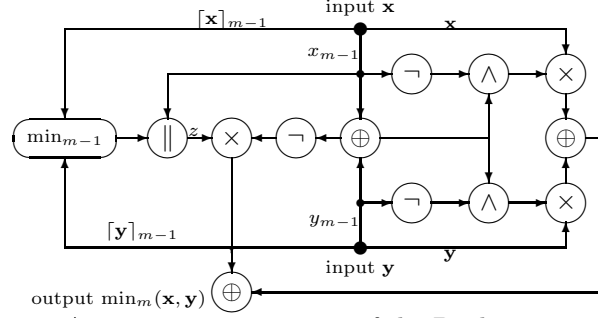


Figure 10: A recursive construction of the Boolean circuit  $\min_m$

and thereby give a recursive description of  $\min_m$  in Figure 10, where  $z = \min_{m-1}([\mathbf{x}]_{m-1}, [\mathbf{y}]_{m-1}) \parallel x_{m-1}$ . Here the multiplying operation “ $\times$ ” has a one-bit input  $a$  and an  $m$ -bit input  $\mathbf{w} = (w_0, w_1, \dots, w_{m-1})$ , and outputs  $(a \wedge w_0, a \wedge w_1, \dots, a \wedge w_{m-1})$ . Thus, the multiplying operation “ $\times$ ” costs  $m$  gates. By Figure 10, we have  $\mathbf{SIZE}(\min_m) = 12 + 13m + \mathbf{SIZE}(\min_{m-1})$  for any  $m \geq 2$ , and hence  $\mathbf{SIZE}(\min_m) = (13m^2 + 37m - 44)/2$ .

## References

- [1] S. Arora and B. Barak, Computational complexity: a modern approach, Cambridge University Press, 2012.
- [2] E. Dubrova: A transformation from the Fibonacci to the Galois NLFSRs, IEEE Trans. Inf. Theory, 55(11):5263–5271, 2009.
- [3] S. W. Golomb: Shift Register Sequences. Laguna Hills, CA, USA: Aegean Park Press, 1981.
- [4] D. H. Green and K. R. Dimond, Nonlinear product-feedback shift registers, Proc. IEE, 117(4):681–686, 1970.
- [5] M. Hell, T. Johansson and W. Meier: The Grain family of stream ciphers, in: New Stream Cipher Designs: The eSTREAM Finalists, in: Lecture Notes in Computer Science, vol. 4986, 2008, pp. 179–190.
- [6] Y. Jiang and D. Lin: On affine subfamilies of Grain-like structure, Des. Codes Cryptogr., 82(3):531–542, 2017. DOI:10.1007/s10623-016-0178-7
- [7] R. Lidl and H. Niederreiter: Finite Fields, Cambridge Univ. Press, Cambridge, U.K., 1997.
- [8] Z. Ma, W. Qi and T. Tian: On the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR, J. Complex., 29(2): 131–181, 2013. DOI:10.1016/j.jco.2012.09.003.
- [9] J. Mykkeltveit, M. Siu and P. Tong: On the cycle structure of some nonlinear shift register sequences, Inf. Control, 43(2):202–215, 1979.
- [10] M. Robshaw and O. Billet (Eds.): New stream cipher designs the eStream finalists, Springer-Verlag, Berlin, Heidelberg, 2008.
- [11] T. Tian and W. Qi: On the largest affine sub-families of a family of NFSR sequences, Designs, Codes Cryptograph., 71(1):163–181, 2014.

- [12] T. Tian and W. Qi: On the density of irreducible NFSRs, *IEEE Trans. Inf. Theory*, 59(6):4006–4012, Jun. 2013.
- [13] T. Tian and W. Qi: On decomposition of an NFSR into a cascade connection of two smaller NFSRs, *Cryptology ePrint Archive*: Report 2014/536.
- [14] J. Zhang, W. Qi, T. Tian and Z. Wang: Further results on the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR, *IEEE Trans. Inf. Theory*, 61(1):645–654, 2015.